НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
КАФЕДРА МАТЕМАТИЧНИХ МЕТОДІВ ЗАХИСТУ ІНФОРМАЦІЇ

«На правах рукопису»
УДК _____

«До захисту допущено»
В.о. завідувача кафедрою
_____ М.М.Савчук
(підпис) (ініціали, прізвище)
“___” _____ 2018р.

Магістерська дисертація

на здобуття ступеня магістра

зі спеціальності 113 Прикладна математика _____
(код і назва)

на тему: «Доказова стійкість блокових шифрів до узагальненого лінійного криптоаналізу на довільних абелевих групах» _____
_____
_____

Виконав (-ла): студент (-ка) __6__ курсу, групи ___ФІ-73мп_____
(шифр групи)

Бахтігозін Всеволод Юрійович _____ _____
(прізвище, ім’я, по батькові) (підпис)

Керівник Яковлєв С.В., доцент кафедри ММЗІ, к.т.н _____ _____
(посада, науковий ступінь, вчене звання, прізвище та ініціали) (підпис)

Консультант _____ _____ _____
(назва розділу) (науковий ступінь, вчене звання, , прізвище, ініціали) (підпис)

Рецензент_____ _____
(посада, науковий ступінь, вчене звання, науковий ступінь, прізвище та ініціали) (підпис)

Засвідчую, що у цій магістерській дисертації немає запозичень з праць інших авторів без відповідних посилань.
Студент _____
(підпис)

Київ – 2018року

Національний технічний університет України
«Київський політехнічний інститут
імені Ігоря Сікорського»
Фізико-технічний інститут
Кафедра математичних методів захисту інформації

Рівень вищої освіти: другий (магістерський) за освітньо–професійною програмою

Спеціальність: 113 «Прикладна математика»

ЗАТВЕРДЖУЮ
В.о. завідувача кафедрою
_____ М.М.Савчук
(підпис) (ініціали, прізвище)
«___»_____201_ р.

ЗАВДАННЯ
на магістерську дисертацію студенту

Бахтігозін Всеволод Юрійович _____
(прізвище, ім'я, по батькові)

1. Тема дисертації «Доказова стійкість блокових шифрів до узагальненого лінійного криптоаналізу на довільних абелевих групах» _____
_____
_____ ,
науковий керівник дисертації Яковлєв С.В., доцент кафедри ММЗІ, к.т.н_____ ,
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом по університету від _____р. № _____

2. Термін подання студентом дисертації _____
3. Об'єкт дослідження: інформаційні процеси в системах криптографічного захисту
_____
4. Предмет дослідження (Вхідні дані – для магістерської дисертації за освітньо–професійною програмою)
моделі та методи лінійного криптоаналізу блокових шифрів
_____
_____
5. Перелік завдань, які потрібно розробити: сформулювати та довести теореми, аналогічні теоремам Ніберг та Парка та ін.; привести приклади застосування одержаних узагальнених теоретичних результатів до сучасних блокових шифрів або їх модифікацій
_____
_____

_____

_____

_____

6. Орієнтовний перелік ілюстративного матеріалу _____

_____

_____

7. Орієнтовний перелік публікацій _____

_____

_____

8. Консультанти розділів дисертації*

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

9. Дата видачі завдання _____

Календарний план

№ з/п	Назва етапів виконання магістерської дисертації	Термін виконання етапів магістерської дисертації	Примітка
1	Узгодження теми з науковим керівником	Вересень 2017	+
2	Опрацювання опублікованих джерел за		
	Тематикою дослідження	Жовтень-грудень 2017	+
3	Формулювання і доведення теореми		
	Аналогічній теоремі Ніберг	Січень-квітень 2018	+
4	Формулювання і доведення теореми		
	Аналогічній теоремі Парка та ін.	Травень-серпень 2018	+
5	Розроблення програмного додатку і		
	Проведення експериментів	Вересень 2018	
6	Оформлення результатів	Жовтень –грудень 2018	+

Студент _____ _____
(підпис) (ініціали, прізвище)

Науковий керівник дисертації _____ _____
(підпис) (ініціали, прізвище)

* Консультантом не може бути зазначено наукового керівника магістерської дисертації.

РЕФЕРАТ

Кваліфікаційна робота містить: 48 стор., 8 рисунки, 3 таблиць, 12 джерел.

Метою даного дослідження є розвинення теорії до узагальненого лінійного криптоаналізу на довільних абелевих групах та побудова методології оцінювання теоретичної та практичної стійкості до даного виду криптоаналізу. Об'єктом дослідження є інформаційні процеси в системах криптографічного захисту. Предметом дослідження є моделі та методи лінійного криптоаналізу блокових шифрів.

Для досягнення данної мети необхідно: сформулювати та довести теореми, аналогічні теоремам Ніберг та Парка та ін.; привести приклади застосування одержаних узагальнених теоретичних результатів до сучасних блокових шифрів або їх модифікацій.

В результаті було сформульовано та доведено теореми про доказову стійкість до узагальненого лінійного криптоаналізу, аналогічні теоремам Ніберг та Парка та ін. про доказовану стійкість схеми Фейстеля та SP-мережі відповідно. Показано, що оцінка стійкості обчислюється через визначені параметри S-блоків, зокрема, максимуми лінійних потенціалів, а також через інші параметри шифрів: індекс розгалуження, кількості раундів. Також було обчислено узагальнені лінійні потенціали S-блоків шифрів SAFER, AES та Калина.

ЛІНІЙНИЙ КРИПТОАНАЛІЗ, ІТЕРАТИВНІ БЛОКОВІ ШИФРИ, УЗАГАЛЬНЕННЯ ЛІНІЙНОГО КРИПТОАНАЛІЗУ

РЕФЕРАТ

Квалификационная работа содержит: 48 стр., 8 рис., 3 таблиц, 12 источников. Целью данной работы является развитие теории обобщенного линейного криптоанализа на произвольных абелевых группах и построение методологии оцениваня теоретической и практической стойкости против данного вида криптоанализа. Объектом исследования являются информационные процессы в системах криптографической защиты. Предметом исследования являются модели и методы линейного криптоанализа блочных шифров.

Для достижения цели необходимо: сформулировать и доказать теоремы, аналогичные теоремам Ниберг и Парка и др.; привести примеры использования полученных обобщенных теоретических результатов к современным блоковым шифрам или их модификациям.

В результате были сформулированы и доказаны теоремы о доказуемой стойкости против обобщенного линейного криптоанализа, аналогичные теоремам Ниберг и Парка и др. о доказуемой стойкости схемы Фейстеля и SP-сети соответственно. Показано, что оценки стойкости вычисляются через определяемые параметры S-блоков, а именно, максимум линейных потенциалов, а также через другие параметры шифров: индекс разветвления, количества раундов. Также были вычислены обобщенные линейные потенциалы S-блоков шифров SAFER, AES и Калина. ЛИНЕЙНЫЙ КРИПТОАНАЛИЗ, ИТЕРАТИВНЫЕ БЛОЧНЫЕ ШИФРЫ, ОБОБЩЕНИЕ ЛИНЕЙНОГО КРИПТОАНАЛИЗА

ABSTRACT

Qualification work contains: 48 pages, 8 fig., 3 tables, 12 references. The goal of this research is development of the theory of generalized linear cryptoanalysis on arbitrary Abelian group and development of methodology of estimation thoretical and practical resistance against this kind of analysis. Object of this work is information processes in systems of cryptograhic security. Subject of this research are models and methods of linear cyptoanalysis of block ciphers.

In order to obtain the goal several tasks must be solved: formulate and prove theorems, analogical to Nyberg and Park et al. theorems; show examples of application obtained generalized theoretical results to modern block ciphers or theirs modifications.

As a result theorems were formulated and proven theorems about resistance against generalized linaear cyptoanalysis, analogical to Nyberg and Park et al.theorems about provable security Feistel scheme and SP-networks respectively. It was shown, that security assessments are computed by means of defined parametres of S-boxes, specificaly, maximal linear potentials, and others cipher parametres: branch index, number of rounds. In addition to it, generalized linear potentials of SAFER, AES and Kalina S-boxes were computed. LINEAR CYPTOANALYSIS, ITERATIVE BLOCK CIPHERS, LINEAR CYPTOANALYSIS GENERALIZATION

ЗМІСТ

ВСТУП

Актуальність дослідження. Лінійний криптоаналіз є одним з найпотужніших методів криптоаналізу симетричних блокових шифрів. Свого часу, національний стандарт шифрування Сполучених Штатів Америки, алгоритм DES був зламаний саме за допомогою лінійного аналізу [8]. З того часу, усі нові шифри перевіряються на стійкість до цього виду аналізу. У свою чергу розвиваються і самі атаки: диференціально-лінійні розпізнавачі, білінійний криптоаналіз, різні види узагальнень класичного лінійного аналізу.

У роботах [6, 5] було запропоновано декілька таких способів узагальнень класичного лінійного криптоаналізу: I-O суми та апроксимації над абелевими групами. Але теорія ще малорозвинена, атаки або застосовні до вузького класу шифрів або існують лише у вигляді теоретичних моделей та сценаріїв, ідсутня загальна методологія оцінювання стійкості алгоритмів шифрування до запропонованих узагальнених типів аналізу.

Метою даного дослідження є розвинення теорії до узгальненого лінійного криптоаналізу на довільних абелевих групах та побудова методології оцінювання теоретичної та практичної стійкості до даного виду криптоаналізу. Для досягнення мети необхідно вирішити такі завдання:

1) провести огляд опублікованих джерел за тематикою дослідження;

2) сформулювати та довести теореми, аналогічні теоремам Ніберг та Парка та ін. про доказовану стійкість схеми Фейстеля та SP-мережі відповідно;

3) привести приклади застосування одержаних узагальнених теоретичних результатів до сучасних блокових шифрів або їх модифікацій;

Об'єктом дослідження є інформаційні процеси в системах

криптографічного захисту.

Предметом дослідження є моделі та методи лінійного криптоаналізу блокових шифрів.

Наукова новизна. Вперше формалізовано теорію доказової стійкості блокових шифрів до узагальненого лінійного криптоаналізу.

Практичне значення. Результати данної роботи довзолять одержувати оцінки теоретичної (доказової) та практичної стійкості шифрів на основі схеми Фейстеля або SP-мережі до узагальненого лінійного криптоаналізу на абелевих групах.

1 НЕОБХІДНІ ПОЗНАЧЕННЯ ТА ОГЛЯД ОПУБЛІКОВАНИХ ДЖЕРЕЛ

На початку цього розділу будуть наведені позначення, необхідні надалі. Далі будуть розглянуті результати досліджень, які так чи інакше використовувались в даній роботі.

1.1 Визначення ітеративного блочного шифру і загальна схема атаки на останній раунд

Позначимо через $\mathbb{M}$ – множину відкритих текстів, $\mathbb{C}$ – множину шифротекстів, $\mathbb{K}$ – множину ключів.

Шифруюче перетворення це функція виду:

$$f : \mathbb{M} \times \mathbb{K} \to \mathbb{C}$$

Розшифровуюче перетворення відповідно визначається наступним чином:

$$f^{-1} : \mathbb{C} \times \mathbb{K} \to \mathbb{M}$$

При цьому повинна виконуватись рівність для всіх $K \in \mathbb{K}$ [1]:

$$f_K^{-1}(f_K(M)) = M$$

Надалі, якщо не вказано інше, будемо вважати, що $\mathbb{M} = \mathbb{C} = V_n$ – множина n-бітних векторів.

Ітеративний r-ранудовий блоковий шифр – перетворення виду

$E : \mathbb{C} \times \mathbb{K}^r \to \mathbb{M}$, яке є композицією простіших шифруючих перетворень:

$$E = f^1_{K_1} \circ f^2_{K_2} \circ ... \circ f^r_{K_r},$$

де $f^i_{K_i}$ – раундове перетворення, K_i – раундовий ключ. Надалі вважаємо, що раундові ключі є незалежними і рівноймовірними.

Якщо $E_K(X) = Y$, то $X = X_0, X_1, ..., X_r = Y$ – проміжні шифротексти, тобто такі, що $X_i = f^i_{K_i}(X_{i-1})$.

На сьогоднішній день існує декілька схем ітеративних блокових шифрів. Найбільш широко використовуються схема Фейстеля і SP мережі.

У схемі Фейстеля елементи вихідної множини V_n розглядаються як пари m-бітних векторів (L, R) $(n = 2m)$. Один раунд схеми Фейстеля визначається наступним чином [2]:

$$F_K(L, R) = (R, L \oplus f_K(R)),$$

де f_K – раундова функція.

Нехай $n = um$, $\bullet$ – операція на V_n. Один раунд SP мережі має вид [2]:

$$F_K = L(S(k(X, K))),$$

де k – функція замішування з ключем, L – лінійне перетворення відносно операції $\bullet$, $S = (s_1, ...s_m)$ – S-блоки, бієктивні нелінійні перетворення виду $s_i : V_u \to V_u$.

Опишемо загальну статистичну атаку на останній раунд. Нехай маємо статистику $R_r(X, X_r)$, розподіл якої є суттєво нерівномірним. Накопичуємо N вхідних текстів X і відповідних їм шифротекстів $Y = E_K(X)$. Для всіх кандидатів $\widetilde{K}_r$ розшифровуємо Y на 1 раунд. Маємо пари (X, X'_{r-1}). Перевіряємо розподіл статистики $\widehat{R}_{r-1}(X, X'_{r-1})$. Якщо був вибраний правильний ключ, то розподіл буде прямувати до R_{r-1}, інакше – до R'_{r+1}, який, за припущенням, буде майже рівноімовірним.

1.2 Класичний лінійний криптоаналіз блокових шифрів

Лінійний криптоаналіз намагається використовувати високоімовірністі появи лінійних виразів, які пов'язують біти відкритого тексту, біти шифротексту і біти раундового ключа. Ця атака є атакою ввідомих відкритих текстів. [3, 8]

Позначимо через $\alpha X \oplus \beta Y \oplus \gamma K = 0$ – лінійна апроксимація, $\Pr(\alpha X \oplus \beta Y \oplus \gamma K = 0) = p$. Ймовірність p повинна суттєво відрізняєтися від $1/2$. Також позначимо через $\varepsilon = 2p - 1$ – кореляція.

Алгоритм M1 полягає в наступному. Нехай маємо шифр E_K, $\alpha X \oplus \beta Y \oplus \gamma K$ – апроксимація з кореляцією $\varepsilon \neq 0$. Далі накопичуємо N пар (X, Y) і підраховумо величину

$$\widetilde{u} = |\{(X, Y) : \alpha X \oplus \beta Y = 0\}| - |\{(X, Y) : \alpha X \oplus \beta Y \neq 0\}|.$$

Покладаємо $\gamma K = [\varepsilon > 0][\widetilde{u} < 0] \vee [\varepsilon < 0][\widetilde{u} > 0]$. Маємо рівняння, за допомогою якого можна знайти один біт ключа. n апроксимаацій з лінійно незалежними векторами γ дозволять знайти відповідно n біт ключа.

На практиці апроксимації шукати складно, тому використовуть алгоритм M2. Нехай $\alpha X \oplus \beta X_{r-1}$ – апроксимація з кореляцією $\varepsilon \neq 0$. Накопичуємо N пар (X, Y). Для всіх кандидатів $\widetilde{K}_1$ зашифровуємо X на один раунд. Підраховуємо величину

$$\widetilde{u}_K = |\{(X, Y) : \alpha X \oplus \beta X_{r-1} = 0\}| - |\{(X, Y) : \alpha X \oplus \beta X_{r-1} = 1\}|.$$

Для істиного ключа K_1 величина $|\widetilde{u}_{K_1}|$ буде приймати найбільше значення.

Також атака на алгоритмі M1 спрацює лише у випадку, коли існує єдина апроксимація (α, β, γ) з кореляцією, яка суттєво відрізняється від 0, що, в загальному випадку, не виконується.

Використання алгоритму M2 замість M1 можливо завдяки узагальненій рівності Парсеваля [4]:

Теорема 1.1.

$$\overline{\sum_K}\left(\Pr_X(\alpha X \oplus \beta Y) - \frac{1}{2}\right)^2 = \overline{\sum_K}\left(\Pr_X(\alpha X \oplus \beta Y \oplus \gamma K) - \frac{1}{2}\right)^2 = \sum_\gamma \left(\Pr_{X,K}(\alpha X \oplus \beta Y \oplus \gamma K) - \frac{1}{2}\right)^2$$

Тобто, можна перейти від усереднених за ключами ймовірностей апроксимацій (α, β, γ), до суми ймовірностей за всіма γ і розглядати спрощенні апроксимації (α, β).

1.3 Оцінки стійкості до класичного лінійного криптоаналізу

Лінійним потенціалом називається величина:

$$LP^f(\alpha, \beta) = \left(\overline{\sum_X}(-1)^{\alpha x \oplus \beta f(x)}\right)^2,$$

де αx та $\beta f(x)$ – скалярні добутки.

Лінійний потенціал, усереднений за ключами називається очікуваним: $ELP^f = \overline{\sum}_K LP^{f_K}$. Визначимо також *максимальний очікуваний потенціал*:

$$MELP^f = \max_{\alpha,\beta \neq 0} ELP^f.$$

Стійкість шифру до лінійного криптоаналізу визначається за допомогою наступних теорем Ніберг [4] та Парка [9].

Теорема 1.2. *Нехай E – схема Фейстеля, f_1, f_2, f_3 – раундові функції, $p_i = MELP^{f_i}$. Тоді $MELP^E \leq \max\{p_1p_2, p_2p_3, p_1p_3\}$.*

Нехай $wt(x)$ – кількість ненульових біт в векторі x. $B(L) = \min_{x \neq 0}(wt(x) + wt(L^*(x)))$ – індекс розгалуження, кількість активних (ненульових) координат у 2 послідовних раундах. L^* – спряжене до L перетворення.

Теорема 1.3. *Нехай E – SP мережа з кількістю раундів $r \geq 2$, то*

$$MELP(E) \leq \max_i(\max_\alpha \sum_\beta (LP^{s_i}(\alpha, \beta))^B, \max_\beta \sum_\alpha (LP^{s_i}(\alpha, \beta))^B),$$

де B – індекс розгалуження лінійного перетворення шифру.

1.4 Узагальнення лінійного криптоаналізу: I-O суми

Узагальнення такого виду було запропоноване у [5]

I-O суммою S^i для i-раунду називається сума за модулем 2 збалансованої бінарної фукнції f_i від X_{i-1} і збалансованою бінарною функцією g_i від X_i:

$$S^i = f_i(X_{i-1}) \oplus g_i(X_i)$$

Функції f_i і g_i називаються відповідно вхідною і вихідною.

I-O суми для послідовних раундів нахиваються *зв'язаними* якщо вихідна функція попереднього раунду співпадає з вхідною функцією наступного. Для r послідовних раундів зі зв'язаними S^i, сума:

$$S^{1..r} = S^1 \oplus S^2 \oplus ... \oplus S^r = g_0(X) \oplus g_r(Y)$$

називається багатораундовою I-O суммою.

Ефективність таких сум вимірюється за допомогою балансу: $I(V) = |2\Pr(V = 0) - 1|$.

Баланс, залежний від ключа, $I(S^{1..r}|k^{1..r})$ I-O суми $S^{1..r}$ це баланс у випадку певного значення ключа $k^{1..r}$. Усереднений баланс $\overline{I}(S^{1..r})$ – баланс

усереднений за всіма значеннями ключа. I-O сума називається єфективною, якщо її баланс суттєво відрізняються від 0.

Базовий алгоритм атаки повністю співпадає зі згаданим вище алгоритмом M2. В цьому випадку також використовується гіпотеза про рандомізацію значень, тобто зашифрування/розшифрування на неправильному ключі зробить розподіл статистики ближчим до рівномірного, та гіпотеза про стохастичну еквівалентність ключів, тобто $I(S^{1..r}|k^{1..r}) \approx \overline{I}(S^{1..r})$ для майже всіх ключів.

1.5 Узагальнення лінійного криптоаналізу: апроксимації над абелевими групами

Наступний матеріл викладений згідно [6]. В цьому підрозділі в першу чергу буде розглянуто необхідний математичний базис, який буде використовуватися далі в данній роботі.

1.5.1 Терміни і позначення

Нехай G – скінчена група порядку n. Тоді $L^2(G)$ – n-мірний векторний простір комплекснозначних функцій f на G.

Скалярний добуток у $L^2(G)$ визначається наступним чином: $(f_1, f_2) = \sum_{a \in G} f_1(a)\overline{f_2(a)}$.

Норма f у $L^2(G)$ визначається як $||f|| = (f, f)^{1/2} = (\sum_a |f(a)|^2)^{1/2}$. А отже $L^2(G)$ – Гільбертов простір.

Характером групи G називається гомоморфізм $\chi : G \leftarrow \mathbb{C}^*$, де $\mathbb{C}^*$ – мультиплікативна група ненульових комплексних чисел. Також

виконуються такі властивості як $\chi(1) = 1$ та $\chi(a_1 a_2) = \chi(a_1)\chi(a_2)$ для всіх $a_1, a_2 \in G$. Очевидно, що $\chi(a)$ – корінь n-го степеня з 1, а отже $\overline{\chi(a)} = \chi^{-1}(a)$.

Добуток двох характерів визначається як $\chi_1\chi_2(a) = \chi_1(a)\chi_2(a)$.

Характер $\mathbb{I}$, визначений як $\mathbb{I}(a) = 1$ для всіх $a \in G$, є нейтральним елементом для цієї операції.

Множина $\widehat{G}$ всіх характерів G є *дуальною групою* для G а також ізоморфною для G.

Надалі будемо користуватись такими властивостями характерів:

1) $\sum_{a \in G} \chi(a) = n \cdot [\chi = 1]$
2) $\sum_{\chi \in \widehat{G}} \chi(a) = n \cdot [a = 1]$
3) $\sum_{a \in G} \chi_1(a)\overline{\chi_2(a)} = n \cdot [\chi_1 = \chi_2]$
4) $\sum_{\chi \in \widehat{G}} \chi(a)\overline{\chi(b)} = n \cdot [a = b]$

де G – скінчена абелева група порядку n, $\widehat{G}$ – відповідна дуальна група.

Перетворенням Фур'є функції $f \in L^2(G)$ є функція $\widehat{f} \in L^2(\widehat{G})$ така що $\widehat{f}(\chi) = (f, \chi)$ для всіх $\chi \in \widehat{G}$. Якщо $\widehat{f} \in L^2(\widehat{G})$ перетворення Фур'є функції $f \in L^2(G)$, то обернене перетворення виконується таким чином:

$$f = \frac{1}{n} \sum_{\chi \in \widehat{G}} \widehat{f}(\chi)\chi$$

Теорема 1.4. *Якщо $\widehat{f} \in L^2(\widehat{G})$ перетворення Фур'є $f \in L^2(G)$, тоді $||\widehat{f}|| = \sqrt{n}||f||$.*

1.5.2 Розпізнавання нерівномірного джерела над скінченою множиною

Покладаємо, що джерело генерує послідовність d незалежних випадкових величин Z^d з розподілу D_s над множиною $\mathbb{Z}$. Задача полягає

в розрізненні випадків $D_s = D$ та $D_s = U$, де U – рівномірний розподіл. Алгоритм, який приймає на вхід вибірку z^d та видає 0 або 1 називається розпізнавачем $\mathbb{D}$. Можливість розпізнавати два розподіли називається *перевагою* розпізнавача і визначається наступним чином

$$Adv^d_{\mathbb{D}} = |\Pr_U(\mathbb{D} = 1) - \Pr_D(\mathbb{D} = 1)|.$$

Супротивник прагне максимізувати цю величину.

Згідно леми Неймана-Пірсона, найкращий розпізнавач базується на принципі максимальної правдоподібності. В його основі лежить порівняння ймовірностей $\Pr_U(z^d)$ та $\Pr_D(z^d)$. Середьноквадратичне відхилення розподілу D над множиною $\mathbb{Z}$ визначається так:

$$\Delta(D) = |\mathbb{Z}| \sum_{z \in \mathbb{Z}} \left(\Pr_D(z) - \frac{1}{|\mathbb{Z}|} \right)^2 = |\mathbb{Z}| \sum_{z \in \mathbb{Z}} \Pr_D(z)^2 - 1$$

В [7] було показано, що перевага найкращого розпізнавача дорівнює:

$$Adv^d_{\mathbb{D}} \approx 1 - 2\Phi(-\sqrt{\lambda}/2),$$

де $\lambda = d \cdot \Delta(D)$ та $\Phi(x) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{x} e^{\frac{u^2}{2}} du$. Звідси можна зробити висновок, що для робочої атаки розмір вибірки повинен бути $d \approx 1/\Delta(D)$.

Використовуючи теорему 1.4, маємо наступне твердження щодо середньоквадратичного відхилення. Для заданого розподілу D над скінченою абелевою групою G порядку n маємо

$$\Delta(D) = n||\Pr_D - \Pr_U||^2 = ||\widehat{\Pr}_D - \widehat{\Pr}_U||^2 = \sum_{\chi \in \widehat{G} \setminus \{\mathbb{I}\}} |\widehat{\Pr}_D(\chi)|^2$$

1.5.3 Узагальнення лінійного потенціалу над абелевими групами

Зазвичай лінійний криптоаналіз джерела бітових строк довжини l полягає в аналізі інформації в кожному рядку за допомогою скалярного добутку з фіксованою маскою $u \in \{0,1\}^l$. Підраховуючи статистичне відхилення цього біту, іноді стає можливо розрізнити ситуації коли $D_s = D$ (відхилення значне) та $D_s = U$(відхилення близько до 0). LP можна узагальнити наступним чином:

$$LP_D(\chi) = |M_D\chi(A)|^2 = |\sum_{a\in G} \chi(a) \Pr_D(a)|^2 = |\widehat{\Pr_D}(\chi)|^2.$$

Таке визначення може використовуватись і для небінарних джерел. Для побудови лінійного розпізнавача введемо наступні поняття:

$$sa(z^d, \chi) = 1/d \sum_{j=1}^{d} \chi(z_j),$$

$$lp(z^d, \chi) = |sa(z^d, \chi)|^2.$$

Порядок лінійного розпізнавача дорівнює порядку відповідного характера χ. Наприклад, коли порядок дорівнює 2, маємо випадок класичного лінійного криптоаналізу.

За законом великих чисел виконується

$$lp(z^d, \chi) \to |M_D\chi(Z)|^2 = LP_D(\chi),$$

де $d \to \infty$. Тобто при великому значенні $lp(z^d, \chi)$ скоріше за всього $D_s = D$, якщо значення близьке до 0 то $D_s = U$. Отже перевага лінійного

розпізнавача визначається оптимізацією виразу відносно τ:

$$Adv^d_{\mathbb{D}}(\chi) = \max_{0<\tau<1} |\Pr_U(lp(Z^d, \chi) < \tau) - \Pr_D(lp(Z^d, \chi) < \tau)|$$

Наступна теорема дозволить оцінити перевагу лінійного розпізнавача в термінах лінійних потенціалів.

Теорема 1.5. *Нехай G – скінчена абелева група і $\chi \in \widehat{G}$. Використовуючи евристичні апроксимації, перевага $Adv^d_{\mathbb{D}}$ лінійного розпізнавача $\mathbb{D}$ має наступну оцінку $Adv^d_{\mathbb{D}} \geq 1 - 2e^{\frac{d}{4}LP_D(\chi)}$ для порядку більше або рівного 3 та $Adv^d_{\mathbb{D}} \geq 1 - 4\Phi(-\frac{1}{2}\sqrt{d \cdot LP_D(\chi)})$ для порядку 2. Теорема виконується при умовах, що d достатньо велике, та при евристичному припущенні рівності матриць коваріацій $lp(Z^d, \chi)$.*

1.5.4 Зв'язок між лінійним і оптимальним розпізнавачами

Теорема 1.6. *Нехай D ймовірнісний розподіл над G. Середньоквадратичне відхилення та лінійні потенціали зв'язані за формулою:*

$$\Delta(D) = \sum_{\chi \in \widehat{G} \setminus \{\mathbb{I}\}} LP_D(\chi)$$

Ця рівність є доволі корисною при спробі покращити лінійний розпізнавач, використовуючи емпіричні закономірності. Якщо існує характер χ такий, що $LP_D(\chi)$ значно перевищує інші лінійні потенціали в попередній рівності, то єдиний характер χ може бути застосований для апроксимації лінійної оболонки. В такому випадку лінійний розпізнавач стає майже оптимальним в сенсі величини вибірки. В якості іншого прикладу розглянемо проблему накопичення лінійних характеристик. В лінійному криптоаналізі, якщо використовувати k незалежних характеристик, то розмір вибірки максимально зменшиться в k разів.

Для середьноквадратичного відхилення існують такі властивості: $\Delta(A+B) \leq \Delta(A)\Delta(B)$ та $\Delta(A||B)+1 \leq (\Delta(A)+1)(\Delta(B)+1)$. Звідси $\Delta(A||B)$ є меншим ніж $\Delta(A)+\Delta(B)$, де A, B – незалежні однаково розподілені случайні величини.

Нехай $LP_D^{\max}$ – максимальний лінійний потенціал за всіма $\chi \in \widehat{G}$ порядку дільника m:

$$LP_D^{\max}(m) = \max_{\chi \in \widehat{G}\setminus\{\mathbb{I}\}, \chi^m = \mathbb{I}} LP_D(\chi)$$

Позначимо через $\circ$ будь-яку можливу операцію на G. Тоді:

$$LP_D^{MAX}(m) = \max_{\circ} LP_D(m)$$

Зауважимо, що LP_D^{MAX} не залежить від структури групи, на відміну від $LP_D^{\max}$.

Якщо m – НСК всіх порядків всіх елементів групи G, і порядок G дорівнює n, то виконуються наступні нерівності:

$$\Delta(D) \leq (n-1)LP_D^{\max}(m),$$

$$\Delta(D) \leq (n-1)LP_D^{MAX}(m).$$

Звідси випливає, що накращий розпізнавач для D має складність за розміром даних щонайменше в $n-1$ раз менше ніж найкращий лінійний розпізнавач.

1.5.5 Оптимальні практичні розпізнавачі

З точки зору розрахунків найкращий розпізнавач описаний вище не можливо реалізувати якщо порядок групи є великим. Розглянемо цей випадок позначивши через множину H великого порядку N і стискаючи

вибірку за допомого проекції:

$$h : H \to G,$$

де G множина порядку $n << N$. Припускаємо, що h збалансоване, а отже $n|N$. Така проекція визначає для випадковох величини $W \in H$ з розподілом $\widetilde{D}_s$, випадкову велчину $h(W) = Z \in G$ з розподілом D.

Лема 1.1. *Нехай H і G скінчені абелеві групи порядку N і n відповідно, такими що $n|N$. Нехай $h : H \to G$ забалансована функція. $\widetilde{D}$ імовірнісний розподіл величини W визначеній на множині H, а D розподіл величини $h(W)$. Тоді $\Delta D \leq \Delta \widetilde{D}$.*

Лема 1.2. *Нехай H і G скінчені абелеві групи порядку N і n відповідно, такими що $n|N$. Нехай $h : H \to G$ сюр'єктивний груповий гомоморфізм. $\widetilde{D}$ імовірнісний розподіл величини W визначеній на множині H, а D розподіл величини $h(W)$. Тоді $\Delta(D) \leq (n-1)LP_{\widetilde{D}}^{\max}(n)$*

Попередній результат можливо застосувати тільки у випадку, коли супротивник зменшує кількість текстів за допомогою групового гомоморфізму, тобто у лінійний спосіб. Дійсно, існують практичні приклади джерел з малими значеннями $LP_{\widetilde{D}}^{\max}$, атаки на які значно спрощується при застосуванні (добре підібраних) негомоморфних проекцій. А отже попередній результат не каже нічого про перевагу довільної проекції.

Теорема 1.7. *Нехай H і G скінчені множини потужності N і n відповідно, такими що $n|N$. Нехай $h : H \to G$ збалансована проекція. $\widetilde{D}$ імовірнісний розподіл величини W визначеній на множині H, а D розподіл величини $h(W)$. Тоді:*

$$\Delta(D) \leq (n-1)LP_{\widetilde{D}}^{MAX}(m).$$

А отже, якщо існує «ефективний» розпізнавач для $\widetilde{D}$, можна використати збаласовану h на «малій» G, $\Delta(D)$ повинно бути великим та

n малим, а отже і $LP_{\widetilde{D}}^{MAX}(n)$ великим.

Висновки до розділу 1

В цьому розділі був розглянутий класичний лінійний криптоаналіз, а саме схеми атаки, їх теоретичне обгрунтування, а також декілька теорем про доказову стійкість класичної схеми Фейстеля та SP-мережі до лінійного криптоаналізу.

Було розглянуто декліька способів узагальнення лінійного криптоаналізу, а саме I-O суми й аналіз на основі абелевих груп. Стосовно останнього виду криптоаналізу також був опрацьований математичний базис.

Теорія для зазначених видів аналізу ще малорозвинена, складно або, навіть, неможливо оцінити стійкість сучасних шифрів. В наступному розділі планується сформулювати і довести теореми аналогічні теоремам Ніберг і Парка для узагальненого лінійного криптоаналізу на абелевих групах.

2 ДОКАЗОВА СТІЙКІСТЬ ДО УЗАГАЛЬНЕНОГО ЛІНІЙНОГО КРИПТОАНАЛІЗУ

В цьому розділі наводяться основні теоретичні викладки даної роботи. А саме, формулювання і доведення теорем про доказову стійкість основних видів блокових шифрів до узагальненого лінійного криптоаналізу

2.1 Схема атаки

Вище були приведені алгоритми M1 та M2 для класичного лінійного криптоаналізу. Для узагальненого лінійного криптоаналізу неможливо адаптувати алгоритм M1, так як випадкові величини виду $\chi(X)$ у загальному випадку не бінарні, а отже неможливо вести поняття аналогічні ε та $\widetilde{u}$.

На відміну від M1, алгоритм M2 майже не змінюється. Супротивник так само накопичує пари відкритих/шифротекстів. Єдина відмінність полягає в способі підрахування лінійних потенціалів.

2.2 Властивості узагальнених лінійних потенціалів

Надалі будемо користуватись наступним визначенням лінійного потенціалу:

$$LP(\alpha,\beta) = |M\left(\chi_\alpha(X)\overline{\chi}_\beta(Y)\right))|^2 = |\overline{\sum}_X(\alpha(X)\overline{\beta}(Y)|,$$

де $Y = E(X)$. У позначенні χ_α індекс α – бітовий вектор. Надалі, якщо не вказано інше, будемо користуватись наступним спрощенням $\chi_\alpha = \alpha$. Характеру $\mathbb{I}$ буде відповідати нейтральний груповий елемент. Будемо вважати, що множина бітових векторів є абелевою групою за операцією додавання за модулем.

Наступні властивості узагальнених лінійних потенціалів доводяться за допомогою властивостей характерів, описаних у розділі 1.

$$LP_f(\alpha, 0) = |\overline{\sum}_X \alpha(X)\overline{\mathbb{I}}(f(X))|^2 = |\overline{\sum}_X \alpha(X)|^2 = [\alpha = \mathbb{I}]$$

$$LP_f(0, \beta) = |\overline{\sum}_X \mathbb{I}(X)\overline{\beta}(f(X))|^2 = |\overline{\sum}_X \overline{\beta}(f(X))|^2 = [\beta = \mathbb{I}],$$

де f – бієкція.

$\forall \beta \in \widehat{G}$ виконується

$$\begin{aligned}
\sum_\alpha LP_f(\alpha, \beta) &= \sum_\alpha |\overline{\sum}_X \alpha(X)\overline{\beta}(f(X))|^2 = \\
&= \sum_\alpha \overline{\sum}_X \alpha(X)\overline{\beta}(f(X)) \cdot \overline{\overline{\sum}_Y \alpha(Y)\overline{\beta}(f(Y))} = \\
&= \sum_\alpha \overline{\sum}_X \alpha(X)\overline{\beta}(f(X)) \cdot \overline{\sum}_Y \overline{\alpha}(Y)\beta(f(Y)) = \\
&\quad \overline{\sum}_{X,Y} \beta(f(Y))\overline{\beta}(f(X)) \sum_\alpha \alpha(X)\overline{\alpha}(Y) = \\
&\quad = \overline{\sum}_{X,Y} \beta(f(Y))\overline{\beta}(f(X))[X = Y] = \\
&\quad = \overline{\sum}_X \beta(f(X))\overline{\beta}(f(X)) = 1
\end{aligned}$$

$\forall \alpha \in \widehat{G}$ виконується

$$\sum_{\beta} LP_f(\alpha,\beta) = \sum_{\beta} |\overline{\sum}_X \alpha(X)\overline{\beta}(f(X))|^2 =$$
$$= \sum_{\beta} \overline{\sum}_X \alpha(X)\overline{\beta}(f(X)) \cdot \overline{\overline{\sum}_Y \alpha(Y)\overline{\beta}(f(Y))} =$$
$$= \sum_{\beta} \overline{\sum}_X \alpha(X)\overline{\beta}(f(X)) \cdot \overline{\sum}_Y \overline{\alpha}(Y)\beta(f(Y)) =$$
$$= \overline{\sum}_{X,Y} \alpha(X)\overline{\alpha}(Y) \sum_{\beta} \beta(f(Y))\overline{\beta}(f(X)) =$$
$$= \overline{\sum}_{X,Y} \alpha(X)\overline{\alpha}(Y)[f(X) = f(Y)] =$$
$$= \overline{\sum}_X \alpha(X)\overline{\alpha}(X) = 1$$

де f – бієкція.

В даній роботі будуть розглядатись шифруючі перетворення виду $f_K(X) = g(X + K)$. Характери будуються так, щоб виконувалась рівність $\chi(X + K) = \chi(X)\chi(K)$, тобто характери є гомоморфізмами. А отже лінійній потенціал операції замішування з ключем буде рівним 1.

Лінійній потенціал вектора S-блоків, в даному випадку, розпадається на добуток потенціалів окремих S-блоків природнім чином.

$$\alpha(X) = \exp\left(\frac{2\pi i}{2^m} \sum_{j=1}^{u} \alpha_j X_j\right) = \prod_{j=1}^{u} \exp\left(\frac{2\pi i}{2^m} \alpha_j X_j\right) = \prod_{j=1}^{u} \alpha_j(X_j),$$

де α_j, X_j – m-бітні вектори, а α, X – u-вимірні вектори з координатами α_j та X_j відповідно. Таким чином лінійний потенціал має наступний вигляд:

$$LP_S(\alpha,\beta) = |\overline{\sum}_X \alpha(X)\beta(S(X))|^2 = |\overline{\sum}_X \prod_{j=1}^{u} \alpha_j(X_j)\beta(s_j(X_j))|^2 =$$
$$= \prod_{j=1}^{u} |\overline{\sum}_{X_j} \alpha_j(X_j)\beta(s_j(X_j))|^2 = \prod_{j=1}^{u} LP_{s_j}(\alpha_j,\beta_j)$$

Аналогічно класичному лінійному криптоаналізу, лінійна

характеристика Ω це послідовність характерів $(\omega_0, \omega_1, ..., \omega_r)$.

Розглянемо наступну величину: $C_f(\alpha, \beta) = \overline{\sum}_X \alpha(X)\overline{\beta}(f(X))$.

Лема 2.1. *Нехай f, g – деякі шифруючі перетворення, $h(x) = g(f(x))$. Тоді $C_h(\alpha, \beta) = \sum_\gamma C_f(\alpha, \gamma)C_g(\gamma, \beta)$.*

Доведення. Розглянемо праву частину умови:

$$\sum_\gamma C_f(\alpha, \gamma)C_g(\gamma, \beta) = \sum_\gamma \left(\overline{\sum}_X \alpha(X)\overline{\gamma}(f(X))\overline{\sum}_Y \gamma(Y)\overline{\beta}(g(Y))\right) =$$
$$= \sum_\gamma \overline{\sum}_{X,Y} \alpha(X)\overline{\gamma}(f(X))\gamma(Y)\overline{\beta}(g(Y)) =$$
$$= \overline{\sum}_{X,Y} \alpha(X)\overline{\beta}(g(Y)) \sum_\gamma \gamma(Y)\overline{\gamma}(f(X)) =$$
$$= \overline{\sum}_{X,Y} \alpha(X)\overline{\beta}(g(Y))[Y = f(X)] =$$
$$= \overline{\sum}_X \alpha(X)\overline{\beta}(g(f(X))) = C_h(\alpha, \beta)$$

□

Використовуючи зазначену лему і матіндукцію можна показати, що:

$$LP_E(\alpha, \beta) = \sum_{\omega_1,...,\omega_{r-1}} \prod_{i=0}^{r-1} LP_{f_i}(\omega_i, \omega_{i+1}),$$

де E – шифр, або деяке складне шифруюче перетворення, f_i – раундові перетворення, $\alpha = \omega_0, \beta = \omega_r$.

2.3 Стійкість шифрів

В розділі 1 згадувалось, що доказова стійкість блокових шифрів до лінійного криптоаналізу грунтується на теоремах Ніберг і Парка. Далі будуть сформульовані і доведені аналогічні теореми для узагальненого лінійного криптоаналізу.

Теорема 2.1. *Нехай* E – 3-*раундова модифікована схема Фейстеля (рис. 2.1),*

$$f_i(X) : V_m \to V_m$$

– *раундове перетворення,*

$$F(X, Y) : V_m \times V_m \to V_m \times V_m$$

– *раунд шифрування. Операція сумування – додавання за модулем.* $p_i = MELP(f_i)$. *Тоді* $LP_E = \max\{p_1p_2, p_2p_3, p_1p_3\}$.

Доведення.

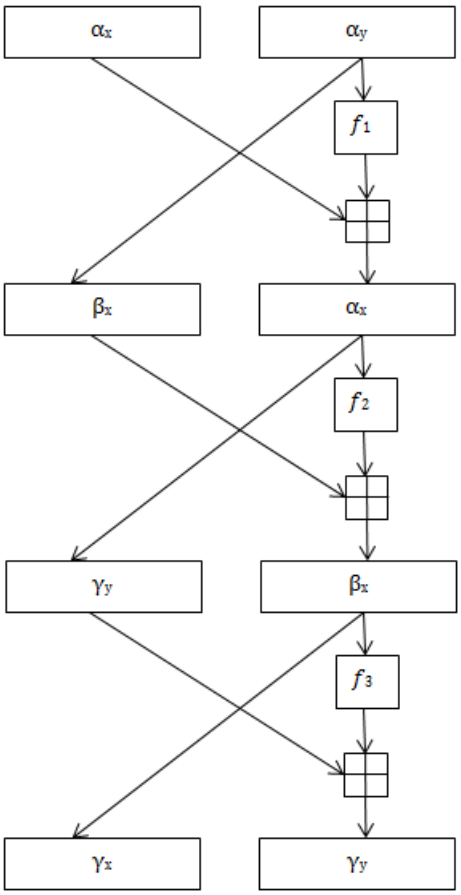

Рисунок 2.1 – 3 раунди модифікованої схеми Фейстеля

Розглянемо лінійний потенціал одного раунда шифрування:

$$\begin{aligned}
LP_F(\alpha,\beta) = |\overline{\sum}_{X,Y}\alpha(X,Y)\overline{\beta}(F(X,Y))|^2 = \\
= \overline{\sum}_{X,Y}\alpha(X,Y)\overline{\beta}(F(X,Y)) = \\
= \overline{\sum}_{X,Y}\alpha_x(X)\alpha_y(Y)\overline{\beta}(Y,X+f(Y)) = \\
= \overline{\sum}_{X,Y}\alpha_x(X)\alpha_y(Y)\overline{\beta}_x(Y)\overline{\beta}_y(X+f(Y)) = \\
= \overline{\sum}_{X}\alpha_x(X)\overline{\beta}_y(X)\cdot\overline{\sum}_{Y}\alpha_y(Y)\overline{\beta}_y(X)\overline{\beta}_y(f(Y)) = \\
= [\alpha_x=\beta_y]\overline{\sum}\chi_{\alpha_y-\beta_x}(Y)\overline{\beta}(f(Y))
\end{aligned}$$

Таким чином лінійний потенціал одного раунду виражається через лінійний потенціал раундового перетворення:

$$LP_F(\alpha,\beta) = [\alpha_x=\beta_y]LP_f(\alpha_y-\beta_x,\beta_y) = LP_f(\alpha_y-\beta_x,\alpha_x)$$

З цього слідує, що 3-раундова характеристика буде мати наступний вигляд: $\Omega(\alpha,\gamma) = (\alpha,\omega_1,\omega_2,\gamma)$, де $\omega_1 = (\beta_x,\alpha_x),\omega_2 = (\gamma_y,\beta_x)$. Лінійні потенціали кожного раунду приймають вигляд:

$$LP_{F_1}(\alpha,\omega_1) = LP_{f_1}(\alpha_y-\beta_x,\alpha_x),$$

$$LP_{F_2}(\omega_1,\omega_2) = LP_{f_2}(\alpha_x-\gamma_y,\beta_x),$$

$$LP_{F_3}(\omega_2,\gamma) = LP_{f_3}(\beta_x-\gamma_x,\gamma_y).$$

Як видно, єдина невідома змінна це β_x. З усього вище наведеного випливає наступне:

$$\begin{aligned}
LP_E(\alpha,\gamma) = \sum_{\omega_1,\omega_2} LP_{F_1}(\alpha,\omega_1)LP_{F_2}(\omega_1,\omega_2)LP_{F_3}(\omega_2,\gamma) = \\
= \sum_{\beta_x} LP_{f_1}(\alpha_y-\beta_x,\alpha_x)LP_{f_2}(\alpha_x-\gamma_y,\beta_x)LP_{f_3}(\beta_x-\gamma_x,\gamma_y)
\end{aligned}$$

Деякі з раундових потенціалів можуть бути рівними 0. Кожен такий випадок потрібно розглянути окремо.

1) Нехай $\alpha_x = 0$, $\alpha_y \neq 0$. В такому випадку маємо $LP_{f_1}(\alpha_y - \beta_x, 0) = [\alpha_y = \beta_x]$. Лінійний потенціал першого раунда буде ненульовим тоді і тільки тоді, коли $\alpha_y = \beta_x$, більш того, він буде рівним 1, а отже $LP_E(\alpha, \gamma) = p_2 p_3$.

2) Нехай $\gamma_y = 0$, $\gamma_x \neq 0$. Тоді $LP_{f_3}(\beta_x - \gamma_x, \gamma_y) = [\beta_x = \gamma_x]$. Аналогічно попередьному випадку $LP_E(\alpha, \gamma) = p_1 p_2$.

3) Нехай $\alpha_x = \gamma_y$. Тоді $LP_{f_2}(\alpha_x - \gamma_y, \beta_x) = [\beta_x = 0]$. Лінійний потенціал другого раунду буде ненульовим, а точніше рівним 1, тоді і тільки тоді коли $\beta_x = 0$, тому $LP_E(\alpha, \gamma) = p_1 p_3$.

4) $\alpha_x \neq \gamma_y, \alpha_x \neq 0, \gamma_y \neq 0$. Оцінимо лінійний потенціал усіх 3 раундів:

$$\begin{aligned} LP_E(\alpha, \gamma) &= \sum_{\omega_1, \omega_2} LP_{F_1}(\alpha, \omega_1) LP_{F_2}(\omega_1, \omega_2) LP_{F_3}(\omega_2, \gamma) = \\ &= \sum_{\beta_x} LP_{f_1}(\alpha_y - \beta_x, \alpha_x) LP_{f_2}(\alpha_x - \gamma_y, \beta_x) LP_{f_3}(\beta_x - \gamma_x, \gamma_y) \leq \\ &\leq p_1 p_3 \sum_{\beta_x} LP_{f_2}(\alpha_x - \gamma_y, \beta_x) \leq p_1 p_3 \end{aligned}$$

□

Теорема 2.2. *Нехай E – 3-раундова модифікована схема Фейстеля, $f_i(X) : V_m \to V_m$ – раундове перетворення, $F(X, Y) : V_m \times V_m \to V_m \times V_m$ – раунд шифрування. Операції сумування чередуються, в непарних раундах додавання за модулем, в парних – різниця за модулем. Це дозволяє зберегти інволютивність. $p_i = MELP(f_i)$. Тоді $LP_E = \max\{p_1 p_2, p_2 p_3, p_1 p_3\}$.*

Доведення. Доведення теореми майже повністю співпадає з попереднім. Розглянемо загальний вигляд лінійного потенціалу парного

раунду.

$$LP_F(\alpha,\beta) = |\overline{\sum}_{X,Y}\alpha(X,Y)\overline{\beta}(F(X,Y))|^2 =$$
$$= \overline{\sum}_{X,Y}\alpha(X,Y)\overline{\beta}(F(X,Y)) =$$
$$= \overline{\sum}_{X,Y}\alpha_x(X)\alpha_y(Y)\overline{\beta}(Y,X-f(Y)) =$$
$$= \overline{\sum}_{X,Y}\alpha_x(X)\alpha_y(Y)\overline{\beta}_x(Y)\overline{\beta}_y(X-f(Y)) =$$
$$= \overline{\sum}_{X}\alpha_x(X)\overline{\beta}_y(X)\cdot\overline{\sum}_{Y}\alpha_y(Y)\overline{\beta}_y(X)\overline{\beta}_y(-f(Y)) =$$
$$= [\alpha_x=\beta_y]\overline{\sum}_{Y}\alpha_y(Y)\overline{\beta}_y(X)\beta_y(f(Y)) =$$
$$= [\alpha_x=\beta_y]\overline{\sum}\chi_{\beta_x-\alpha_y}(Y)\overline{\beta}(f(Y))$$
$$\Rightarrow LP_F(\alpha,\beta) = [\alpha_x=\beta_y]LP_f(\beta_x-\alpha_y,\beta_y) =$$
$$= LP_f(\beta_x-\alpha_y,\alpha_x)$$

Подальше доведення залишається без змін. □

Теореми 2.1 та 2.2 виражають стійкість 3-х раундів шифрування за модифікованими схемами Фейстеля, через лінійні потенціали раундових перетворень.

Теорема 2.3. *Нехай $E = S(L(S))$, де $S = (s_1, s_2, ..., s_q)$, $s_i : V_m \to V_m$ – вектор S-блоків, $L : (V_m)^q \to (V_m)^q$ – лінійне перетворення. $B(L) = B$ – індекс розгалуження. Тоді виконується рівність: $\forall\alpha\forall\beta \neq 0$:*

$$LP_E(\alpha,\beta) \le \max_i(\max_{\alpha_i}(\sum_{\beta_i}(\operatorname{ord}\beta_i - 1)(LP_{s_i}(\alpha_i,\beta_i))^B),$$
$$\max_{\beta_i}(\sum_{\alpha_i}(\operatorname{ord}\alpha_i - 1)(LP_{s_i}(\alpha_i,\beta_i))^B))$$

Доведення. Розпишемо лінійний потенціал:

$$LP_E(\alpha,\beta) = \sum_{\gamma}\left(\prod_{i=1}^{m}LP_{s_i}(\alpha_i,\gamma_i)\prod_{j=1}^{m}LP_{s_j}(\widetilde{\gamma}_j,\beta_j)\right)$$

де $\widetilde{\gamma} = L^*(\gamma)$, L^* – спряжене перетворення. Позначимо $wt(\alpha) = wt(\gamma) = v$,

$wt(\beta) = wt(\widetilde{\gamma}) = u$, $v \geq u$. У випадку коли $v \leq u$ доведення буде повністю аналогічним. Нехай ненульові координати α, γ мають номери з 1 по v; $\beta, \widetilde{\gamma}$ – з 1 по u. Тоді:

$$LP_E(\alpha, \beta) = \sum_{\gamma} \left(\prod_{i=1}^{v} LP_{s_i}(\alpha_i, \gamma_i) \prod_{j=1}^{u} LP_{s_j}(\widetilde{\gamma}_j, \beta_j)) \right)$$

Розглянемо два випадки:

1) $v + u = B$. Для всіх можливих γ, при деякому i, кожне γ_i зустрічається не більше $w = \operatorname{ord} \gamma_i$. Якщо це не так і існують вектори $\gamma^1, \gamma^2, ..., \gamma^{w+1}$ з однаковими значеннями i-тої координати, тоді вектор $\gamma' = \gamma^1 + \gamma^2 + ... + \gamma^{w+1}$ буде мати $wt(\gamma') < v$, а отже й $wt(\gamma') + wt(L(\gamma')) < u + v = B$, що протирічить умові.
За наслідком з узагальненої нерівності Коші-Буняковського:

$$LP_E(\alpha, \beta) = \sum_{\gamma} \left(\prod_{i=1}^{v} \prod_{j=1}^{u} LP_{s_i}(\alpha_i, \gamma_i) \cdot LP_{s_j}(\widetilde{\gamma}_j, \beta_j)) \right) =$$

$$= \max_{i,j} (\sum_{\gamma_i} (\operatorname{ord} \gamma_i - 1)(LP_{s_i}(\alpha_i, \gamma_i))^B, \sum_{\widetilde{\gamma}_j} (\operatorname{ord} \widetilde{\gamma}_j - 1)(LP_{s_i}(\widetilde{\gamma}_j, \beta_j))^B) \leq$$

$$\leq \max_{i,j} (\max_{\alpha_i} \sum_{\gamma_i} (\operatorname{ord} \gamma_i - 1)(LP_{s_i}(\alpha_i, \gamma_i))^B, \max_{beta_j} \sum_{\widetilde{\gamma}_j} (\operatorname{ord} \widetilde{\gamma}_j - 1)(LP_{s_i}(\widetilde{\gamma}_j, \beta_j))^B)$$

2) $v + u > B$. Неможливо нічого стверджувати про кількість γ_i при фіксованому i. Тому зафіксуємо певні значення γ_i при $B - u + 1 \leq i \leq v$. За аналогією у випадку 1), ненульові координати, що залишились $i \leq B - u$, будуть приймати кожне значення менше ніж власний порядок

разів. Маємо:

$$LP_E(\alpha,\beta) \leq$$
$$\leq \sum_{\gamma_{B-u+1}} LP_{s_{B-u+1}}(\alpha_{B-u+1},\gamma_{B-u+1}) \ldots \sum_{\gamma_v} LP_{s_v}(\alpha_v,\gamma_v) \times$$
$$\times \sum_{\gamma_1,\ldots\gamma_{B-u}} \prod_{i=1}^{B-u} \prod_{j=1}^{u} LP_{s_i}(\alpha_i,\gamma_i) LP_{s_j}(\widetilde{\gamma}_j,\beta_j) \leq$$
$$\leq \sum_{\gamma_{B-u+1}} LP_{s_{B-u+1}}(\alpha_{B-u+1},\gamma_{B-u+1}) \ldots \sum_{\gamma_v} LP_{s_v}(\alpha_v,\gamma_v) \times$$
$$\times \max_{i,j}\Big(\max_{\alpha_i} \sum_{\gamma_i} (\operatorname{ord}\gamma_i - 1)(LP_{s_i}(\alpha_i,\gamma_i)))^B, \max_{beta_j} \sum_{\widetilde{\gamma}_j} (\operatorname{ord}\widetilde{\gamma}_j - 1)(LP_{s_i}(\widetilde{\gamma}_j,\beta_j)))^B\Big) \leq$$
$$\leq \max_{\beta_j} \sum_{\widetilde{\gamma}_j} (\operatorname{ord}\widetilde{\gamma}_j - 1)(LP_{s_i}(\widetilde{\gamma}_j,\beta_j))^B)$$

□

Теорема 2.3 виражає стійкість 2-х раундової SP-мережі через обчислювані параметри S-блоків і лінійного перетворення.

Висновки до розділу 2

В цьому розділі були сформульовані та доведені теореми про доказову стійкість модифікованих схем Фейстеля та SP-мережі до узагальненого лінійного криптоаналізу.

3 ОЦІНКИ СТІЙКОСТІ ТА ПРИКЛАДИ ВИКОРИСТАННЯ ТЕОРЕМ

В цьому розділі буде обчислено таблиці розподілів узагальених лінійні потенціалів для S-блоків деяких шифрів. На основі одержаних розрахункових результатів будуть побудовані оцінки стійкості шифрів стійкість шифрів, побудованих на модифікованій схемі Фейстеля та SP-мережі.

3.1 Розрахунки узагальнених лінійних потенціалів

В ході практичної частини були підраховані узагальнені лінійні потенціали S-блоків таких шифрів як SAFER, AES та ДСТУ 7624 : 2014 «Калина». S-блоки шифру SAFER являють собою наступні операції

$$s(x) = (45^x \bmod 257) \bmod 256,$$

$$s^{-1}(x) = (\log_{45} x \bmod 257) \bmod 256,$$

де $s(x) = 0$ при $x = 128$ та $s^{-1}(x) = 128$ при $x = 0$ [10]. SAFER в подальшому буде досліджений більш детально, оскільки лінійне перетворення цього шифру є лінійним відносно операції модульного додавання, а S-блоки теоретично мають мінімально можливі ймовірності диференціалів за операцією додавання за модулем.

Шифр AES має єдиний S-блок: кожен байт стану шифрування представляється як елемент $\mathbb{F}_{2^8}$, до якого обчислюється обернений елемент і до результату застосовується спеціально підібране зафіксоване перетворення [11]. Національний стандарт шифрування« Калина» має 4

S-блоки, які не мають аналітичного представлення [12]. Усі зазначені S-блоки приведені у лістингу програми у додатку.

В таблиці 3.1 представлені максимальні значення узагальнених лінійних потенціалів S-блоків зазначених вище шифрів:

$$maxLP = \max_{\alpha,\beta} 2^{2n} LP(\alpha, \beta),$$

де n – розмір S-блоків. В данному випадку всі S-блоки мають розмір 8 біт.

Таблиця 3.1 – Максимальні значення узагальнених лінійних потенціалів S-блоків

SAFER	SAFER(inv)	AES	Калина1	Калина2	Калина3	Калина4
$1804,89$	$1804,89$	$2649,60$	$2174,36$	$2795,78$	$3310,61$	$2475,73$

Також були підраховані функції розподілу:

$$F(x) = |(\alpha, \beta) : 2^{2n} LP(\alpha, \beta) < x|$$

Графіки функцій розподілу представлені на рис. 3.1, Б.1 – Б.6

3.2 Оцінки стійкості деяких шифрів до узагальненого виду криптоаналізу

Шифр SAFER++ є SP-мережою з 16-байтним блоком шифрування. Лінійне перетворення має наступний вигляд: перестановка байт, байти діляться на групи по 4 байти, до кожної такої групи застосовується псевдоперетворення Адамара, ще одна перестановка байт і ще одне псевдоперетворення Адамара. Лінійне перетворення має індекс

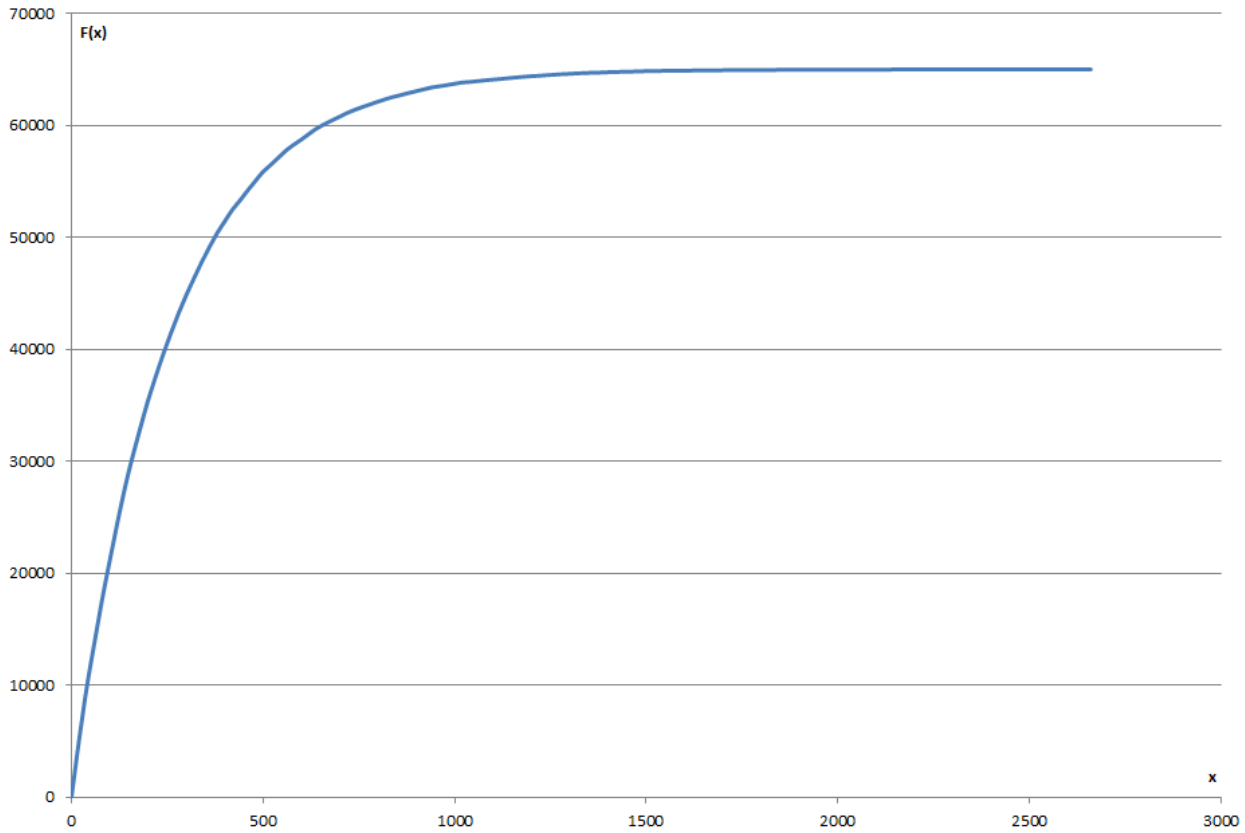

Рисунок 3.1 – Графік функціїї розподілу лінійних потенціалів AES. По осі X – значення потенціалу, по Y – кількість таких потенціалів

розгалуження 5. Додавання ключа відбувається за операцією модульного та побітового додавання побайтово.

Розглянемо модифікації шифру SAFER, які полягають у

– заміні усіх операцій побітового додавання с байтами ключа на операції додавання за модулем 256,

– заміні лінійного перетворення на інші матричні перетворення над $\mathbb{Z}_{256}$.

Оскільки загальна оцінка стійкості залежить лише від індексу розгалуження лінійного перетворення, для аналізу можна просто зафіксувати значення самого індексу, не описуючи власне перетворення. Перевіримо індекси розгалуження від 3 до 10 за допомогою теореми 2.3. При значенні індексу рівному 2, оцінка, згідно теоремі, більша 1, а отйже є неадекватною і нічого каже про стійкість такої модифікації шифру.

Як і очікувалось, чим більше індекс розгалуження, тим вища стійкість

Таблиця 3.2 – Дослідження стійкості SAFER++

B	3	4	5	6	7	8	9	10
LP	$2^{-4,56}$	$2^{-10,37}$	2^{-16}	$2^{-21,49}$	$2^{-26,88}$	$2^{-32,2}$	$2^{-37,47}$	$2^{-42,72}$

шифру до аналізу, але навіть при максимальному значенні індекса шифр не можна вважати гарантовано стійким, оскільки на сьогоднішній день шифри вважаються гарантовано стійкими при значенні 2^{-80}.

Розгляенмо простий шифр, в основі якого лежить модифікована схема Фейстеля, описана в розділі 2. Розмір блоку шифрування покладемо $n = 16$ біт, а в якості раундового перетворення візьмемо S-блоки шифрів SAFER, AES і Калина. Раундовий ключ вводится за операцією додавання за модулем. Дослідимо стійкість такого шифру до узагальненого лінійного криптоаналізу (таб. 3.3).

Таблиця 3.3 – Стійкість схеми Фейстеля

SAFER	SAFER(inv)	AES	Калина1	Калина2	Калина3	Калина4
$2^{-10,36}$	$2^{-10,36}$	$2^{-9,26}$	$2^{-9,82}$	$2^{-9,1}$	$2^{-8,61}$	$2^{-9,46}$

Як видно з таблиці, такий шифр є зовсім не стійким до узагальненого лінійного криптоаналізу.

Висновки до розділу 3

В цьому розділі були експериментально досліджені стійкості S-блоків таких шифрів як SAFER, AES і Калина. Також були наведені приклади застосувань основних теорем данної роботи на модифікованому шифрі SAFER++ і формальному шифрі на схемі Фейстеля.

ВИСНОВКИ

В ході даного дослідження було розглянуто опубліковані результати щодо стійкості шифрів до класичного лінійного криптоаналізу, способів узагальнення лінійного криптоаналізу.

Було розглянуто поняття узагальненої лінійної апроксимації булевої функції та узагальнених лінійних потенціалів, виражені через характери певної абелевої групи, та досліджено їх властивості. Було сформульовано та доведено теореми про доказову стійкість до узагальненого лінійного криптоаналізу, аналогічні теоремам Ніберг та Парка та ін. про доказовану стійкість схеми Фейстеля та SP мережі відповідно.

Показано, що (як і для класичного криптоаналізу) оцінка стійкості обчислюється через визначені параметри S-блоків, зокрема, максимуми узагальнених лінійних потенціалів, а також через інші параметри шифрів: індексу розгалуження, кількості раундів. Також було обчислено узагальнені лінійні потенціали S-блоків шифрів SAFER, AES та Калина. З усіх представлених, оберенений S-блок шифру SAFER має найменше значення максимального лінійного потенціалу.

Іншим завданням було розглянути застосування доведенних теорем на прикладах. Після проведеного аналізу неможливо нічого стверджувати про стійкість розглянутих шифрів. Можна сказати, зо отримані оцінки гарантованої складності атаки не показують достатній рівень стійкості, потрібно проводити додатковий аналіз. Модифікований шифр SAFER, наприклад, має найкращу оцінку $2^{-42,72}$, що не достатньо, щоб вважати його гарантовано стійким.

До напрямків подальших досліджень можна віднести інші способи узагальнення лінійного криптоаналізу, аналіз абелевих груп на інших операціях (наприклад, множення за модулем).

ПЕРЕЛІК ПОСИЛАНЬ

1. Schneier B. Applied cryptography (2nd ed.): protocols, algorithms, and source code in C. John Wiley & Sons, Inc. New York, NY, USA @1995 ISBN:0-471-11709-9

2. Feistel H. Some cryptographic techniques for machine to machine data communications / H. Feistel, W. A. Notz, and J. L. Smith // Proceedings of the IEEE. – Vol. 63. – #11. – 1975. – pp. 1545-1554.

3. Heys Howard M. A Tutorial on Linear and Differential Cryptanalysis [електронний ресурс] / Howard M. Heys. – Режим доступу : http://www.engr.mun.ca/~howard/PAPERS/ldc_tutorial.pdf

4. Nyberg Kaisa. Linear Approximation of Block Ciphers / Kaisa Nyberg // EUROCRYPT'94. – Lecture Notes in Computer Science, vol. 950. – Springer Verlag, 1994.

5. Harpes et al. A Generalization of Linear Cryptanalysis and the Applicability of Matsui's Piling-up Lemma. Carlo Harpes, Gerhard G. Kramer, James L. Massey. Swiss Federal Institute of Technology, Signal and Info. Proc. Lab., CH-8092 Zurich. May 19, 1995

6. Baignères T., Stern J., Vaudenay S. (2007) Linear Cryptanalysis of Non Binary Ciphers. In: Adams C., Miri A., Wiener M. (eds) Selected Areas in Cryptography. SAC 2007. Lecture Notes in Computer Science, vol 4876. Springer, Berlin, Heidelberg

7. T. Baign‘eres, P. Junod, and S. Vaudenay. How far can we go beyond linear crypt- analysis? In Advances in Cryptology - Asiacrypt'04, volume 3329 of LNCS, pages 432–450. Springer-Verlag, 2004.

8. Matsui M. (1994) Linear Cryptanalysis Method for DES Cipher. In: Helleseth T. (eds) Advances in Cryptology — EUROCRYPT '93. EUROCRYPT 1993. Lecture Notes in Computer Science, vol 765. Springer, Berlin, Heidelberg

9. Park S. Improving the upper bound on the maximum differential and the maximum linear hull probability for the SPN structures and AES / S. Park,

J. Sung, S. Lee, J. Lim // Fast Software Encryption. – FSE'03, Proceedings. – Springer Verlag, 2003. – P. 247 – 260.

10. J. L. Massey, G. Khachatrian, and M. K. Kuregian, "Nomination of SAFER++ as candidate algorithm for the New European Schemes for Signatures, Integrity, and Encryption (NESSIE)." Primitive submitted to NESSIE by Cylink Corp., Sept. 2000.

11. Joan Daemen. AES Proposal: Rijndael [електронний ресурс] / Joan Daemen, Vincent Rijmen – Режим доступу :https://csrc.nist.gov/CSRC/media/Projects/Cryptographic-Standards-and-Guidelines/documents/aes-development/Rijndael-ammended.pdf

12. A New Encryption Standard of Ukraine: The Kalyna Block Cipher [електронний ресурс] /Roman Oliynykov, Ivan Gorbenko, Oleksandr Kazymyrov, Victor Ruzhentsev, Oleksandr Kuznetsov, Yurii Gorbenko, Oleksandr Dyrda, Viktor Dolgov, Andrii Pushkaryov, Ruslan Mordvinov, Dmytro Kaidalov – Режим доступу :https://eprint.iacr.org/2015/650.pdf

ДОДАТОК А ТЕКСТИ ПРОГРАМ

Header.h

```
#include <complex>
#include <vector>

using permutation = std::vector<unsigned long long>;
using cmplx = std::complex<double>;
using table = std::vector<std::vector<double>>;

table experiment(const permutation &prm, unsigned n);
void distribution(const table &data, unsigned n);
double parkTheorem(const table &potentials, unsigned n,  unsigned brnchIndx);
```

Source.cpp

```
#include "Header.h"
#include <fstream>

const std::vector<int> ord{
  0, 256, 128, 256, 64, 256, 128, 256, 32, 256, 128, 256, 64, 256, 128, 256,
  16, 256, 128, 256, 64, 256, 128, 256, 32, 256, 128, 256, 64, 256, 128, 256,
  8, 256, 128, 256, 64, 256, 128, 256, 32, 256, 128, 256, 64, 256, 128, 256,
  16, 256, 128, 256, 64, 256, 128, 256, 32, 256, 128, 256, 64, 256, 128, 256,
  4, 256, 128, 256, 64, 256, 128, 256, 32, 256, 128, 256, 64, 256, 128, 256,
  16, 256, 128, 256, 64, 256, 128, 256, 32, 256, 128, 256, 64, 256, 128, 256,
  8, 256, 128, 256, 64, 256, 128, 256, 32, 256, 128, 256, 64, 256, 128, 256,
  16, 256, 128, 256, 64, 256, 128, 256, 32, 256, 128, 256, 64, 256, 128, 256,
  2, 256, 128, 256, 64, 256, 128, 256, 32, 256, 128, 256, 64, 256, 128, 256,
  16, 256, 128, 256, 64, 256, 128, 256, 32, 256, 128, 256, 64, 256, 128, 256,
  8, 256, 128, 256, 64, 256, 128, 256, 32, 256, 128, 256, 64, 256, 128, 256,
  16, 256, 128, 256, 64, 256, 128, 256, 32, 256, 128, 256, 64, 256, 128, 256,
  4, 256, 128, 256, 64, 256, 128, 256, 32, 256, 128, 256, 64, 256, 128, 256,
  16, 256, 128, 256, 64, 256, 128, 256, 32, 256, 128, 256, 64, 256, 128, 256,
  8, 256, 128, 256, 64, 256, 128, 256, 32, 256, 128, 256, 64, 256, 128, 256,
  16, 256, 128, 256, 64, 256, 128, 256, 32, 256, 128, 256, 64, 256, 128, 256 };
table experiment(const permutation &prm, unsigned n){
  const int size(1 << n);
  const int mod(size - 1);
  const double pi = std::acos(-1);
  cmplx sum(0, 0);
  const cmplx e = std::exp(cmplx(0, 1) * pi * 2.0 / (double)size);
  table data(size, std::vector<double>(size, 0));

  for (unsigned a = 1; a < size; a++) {
```

```
    for (unsigned b = 1; b < size; b++)   {
      for (unsigned x = 0; x < size; x++)     {
        sum += std::pow(e, (a*x - b * prm[x]) & mod);
      }
      data[a][b] = std::norm(sum);
      sum = 0;
    }
  }
  std::ofstream out("data.txt");
  for (int i = 1; i < size; i++)  {
    out << ' ' << i;
  }
  out << std::endl;
  for (int a = 1; a < size; a++)  {
    out << a << ' ';
    for (int b = 1; b < size; b++)    {
      out << data[a][b] << ' ';
    }
    out << std::endl;
  }
  out.close();
  return data;
}
void distribution(const table &data, unsigned n){
  const int absval(1 << 2*n);
  const int size(1 << n);
  int precision(20);
  std::vector<int> dstrb(absval / precision, 0);
  int j;
  int end(3400);
  dstrb[0] = 0;
  for (int i = precision; i < end; i+=precision)  {
    j = i / precision;
    for (int r = 1; r < size; r++)    {
      for (int c = 1; c < size; c++)      {
        dstrb[j] += static_cast<int>(data[r][c] < i);
      }
    }
  }
  std::ofstream out("distribution.txt");
  for (auto d : dstrb)
    out << d << ' ';
  out.close();
}
double parkTheorem(const table &potentials, unsigned n, unsigned brnchIndx){
```

```
  const int size(1 << n);
  const int denum(size*size);
  double sum1(0), tmp;
  for (int a = 1; a < size; a++) {
    tmp = 0;
    for (int b = 1; b < size; b++)    {
      tmp += (ord[b] - 1)*pow(potentials[a][b], brnchIndx);
    }
    if (tmp > sum1)
      sum1 = tmp;
  }

  double sum2(0);
  for (int b = 1; b < size; b++){
    tmp = 0;
    for (int a = 1; a < size; a++)    {
      tmp += (ord[a] - 1)*pow(potentials[a][b], brnchIndx);
    }
    if (tmp > sum2)
      sum2 = tmp;
  }
  return ((sum1 > sum2) ? sum1 : sum2) / pow(denum, brnchIndx);
}
```

main.cpp

```
#include "Header.h"
#include <iostream>

permutation saferSB{
  0x01, 0x2d, 0xe2, 0x93, 0xbe, 0x45, 0x15, 0xae, 0x78, 0x03, 0x87, 0xa4, 0xb8, 0x38, 0xcf, 0x3f,
  0x08, 0x67, 0x09, 0x94, 0xeb, 0x26, 0xa8, 0x6b, 0xbd, 0x18, 0x34, 0x1b, 0xbb, 0xbf, 0x72, 0xf7,
  0x40, 0x35, 0x48, 0x9c, 0x51, 0x2f, 0x3b, 0x55, 0xe3, 0xc0, 0x9f, 0xd8, 0xd3, 0xf3, 0x8d, 0xb1,
  0xff, 0xa7, 0x3e, 0xdc, 0x86, 0x77, 0xd7, 0xa6, 0x11, 0xfb, 0xf4, 0xba, 0x92, 0x91, 0x64, 0x83,
  0xf1, 0x33, 0xef, 0xda, 0x2c, 0xb5, 0xb2, 0x2b, 0x88, 0xd1, 0x99, 0xcb, 0x8c, 0x84, 0x1d, 0x14,
  0x81, 0x97, 0x71, 0xca, 0x5f, 0xa3, 0x8b, 0x57, 0x3c, 0x82, 0xc4, 0x52, 0x5c, 0x1c, 0xe8, 0xa0,
  0x04, 0xb4, 0x85, 0x4a, 0xf6, 0x13, 0x54, 0xb6, 0xdf, 0x0c, 0x1a, 0x8e, 0xde, 0xe0, 0x39, 0xfc,
  0x20, 0x9b, 0x24, 0x4e, 0xa9, 0x98, 0x9e, 0xab, 0xf2, 0x60, 0xd0, 0x6c, 0xea, 0xfa, 0xc7, 0xd9,
  0x00, 0xd4, 0x1f, 0x6e, 0x43, 0xbc, 0xec, 0x53, 0x89, 0xfe, 0x7a, 0x5d, 0x49, 0xc9, 0x32, 0xc2,
  0xf9, 0x9a, 0xf8, 0x6d, 0x16, 0xdb, 0x59, 0x96, 0x44, 0xe9, 0xcd, 0xe6, 0x46, 0x42, 0x8f, 0x0a,
  0xc1, 0xcc, 0xb9, 0x65, 0xb0, 0xd2, 0xc6, 0xac, 0x1e, 0x41, 0x62, 0x29, 0x2e, 0x0e, 0x74, 0x50,
  0x02, 0x5a, 0xc3, 0x25, 0x7b, 0x8a, 0x2a, 0x5b, 0xf0, 0x06, 0x0d, 0x47, 0x6f, 0x70, 0x9d, 0x7e,
  0x10, 0xce, 0x12, 0x27, 0xd5, 0x4c, 0x4f, 0xd6, 0x79, 0x30, 0x68, 0x36, 0x75, 0x7d, 0xe4, 0xed,
  0x80, 0x6a, 0x90, 0x37, 0xa2, 0x5e, 0x76, 0xaa, 0xc5, 0x7f, 0x3d, 0xaf, 0xa5, 0xe5, 0x19, 0x61,
  0xfd, 0x4d, 0x7c, 0xb7, 0x0b, 0xee, 0xad, 0x4b, 0x22, 0xf5, 0xe7, 0x73, 0x23, 0x21, 0xc8, 0x05,
  0xe1, 0x66, 0xdd, 0xb3, 0x58, 0x69, 0x63, 0x56, 0x0f, 0xa1, 0x31, 0x95, 0x17, 0x07, 0x3a, 0x28 };
```

```
permutation saferSBI{
  0x80, 0x00, 0xb0, 0x09, 0x60, 0xef, 0xb9, 0xfd, 0x10, 0x12, 0x9f, 0xe4, 0x69, 0xba, 0xad, 0xf8,
  0xc0, 0x38, 0xc2, 0x65, 0x4f, 0x06, 0x94, 0xfc, 0x19, 0xde, 0x6a, 0x1b, 0x5d, 0x4e, 0xa8, 0x82,
  0x70, 0xed, 0xe8, 0xec, 0x72, 0xb3, 0x15, 0xc3, 0xff, 0xab, 0xb6, 0x47, 0x44, 0x01, 0xac, 0x25,
  0xc9, 0xfa, 0x8e, 0x41, 0x1a, 0x21, 0xcb, 0xd3, 0x0d, 0x6e, 0xfe, 0x26, 0x58, 0xda, 0x32, 0x0f,
  0x20, 0xa9, 0x9d, 0x84, 0x98, 0x05, 0x9c, 0xbb, 0x22, 0x8c, 0x63, 0xe7, 0xc5, 0xe1, 0x73, 0xc6,
  0xaf, 0x24, 0x5b, 0x87, 0x66, 0x27, 0xf7, 0x57, 0xf4, 0x96, 0xb1, 0xb7, 0x5c, 0x8b, 0xd5, 0x54,
  0x79, 0xdf, 0xaa, 0xf6, 0x3e, 0xa3, 0xf1, 0x11, 0xca, 0xf5, 0xd1, 0x17, 0x7b, 0x93, 0x83, 0xbc,
  0xbd, 0x52, 0x1e, 0xeb, 0xae, 0xcc, 0xd6, 0x35, 0x08, 0xc8, 0x8a, 0xb4, 0xe2, 0xcd, 0xbf, 0xd9,
  0xd0, 0x50, 0x59, 0x3f, 0x4d, 0x62, 0x34, 0x0a, 0x48, 0x88, 0xb5, 0x56, 0x4c, 0x2e, 0x6b, 0x9e,
  0xd2, 0x3d, 0x3c, 0x03, 0x13, 0xfb, 0x97, 0x51, 0x75, 0x4a, 0x91, 0x71, 0x23, 0xbe, 0x76, 0x2a,
  0x5f, 0xf9, 0xd4, 0x55, 0x0b, 0xdc, 0x37, 0x31, 0x16, 0x74, 0xd7, 0x77, 0xa7, 0xe6, 0x07, 0xdb,
  0xa4, 0x2f, 0x46, 0xf3, 0x61, 0x45, 0x67, 0xe3, 0x0c, 0xa2, 0x3b, 0x1c, 0x85, 0x18, 0x04, 0x1d,
  0x29, 0xa0, 0x8f, 0xb2, 0x5a, 0xd8, 0xa6, 0x7e, 0xee, 0x8d, 0x53, 0x4b, 0xa1, 0x9a, 0xc1, 0x0e,
  0x7a, 0x49, 0xa5, 0x2c, 0x81, 0xc4, 0xc7, 0x36, 0x2b, 0x7f, 0x43, 0x95, 0x33, 0xf2, 0x6c, 0x68,
  0x6d, 0xf0, 0x02, 0x28, 0xce, 0xdd, 0x9b, 0xea, 0x5e, 0x99, 0x7c, 0x14, 0x86, 0xcf, 0xe5, 0x42,
  0xb8, 0x40, 0x78, 0x2d, 0x3a, 0xe9, 0x64, 0x1f, 0x92, 0x90, 0x7d, 0x39, 0x6f, 0xe0, 0x89, 0x30};

permutation aesSB{
  0x63, 0x7c, 0x77, 0x7b, 0xf2, 0x6b, 0x6f, 0xc5, 0x30, 0x01, 0x67, 0x2b, 0xfe, 0xd7, 0xab, 0x76,
  0xca, 0x82, 0xc9, 0x7d, 0xfa, 0x59, 0x47, 0xf0, 0xad, 0xd4, 0xa2, 0xaf, 0x9c, 0xa4, 0x72, 0xc0,
  0xb7, 0xfd, 0x93, 0x26, 0x36, 0x3f, 0xf7, 0xcc, 0x34, 0xa5, 0xe5, 0xf1, 0x71, 0xd8, 0x31, 0x15,
  0x04, 0xc7, 0x23, 0xc3, 0x18, 0x96, 0x05, 0x9a, 0x07, 0x12, 0x80, 0xe2, 0xeb, 0x27, 0xb2, 0x75,
  0x09, 0x83, 0x2c, 0x1a, 0x1b, 0x6e, 0x5a, 0xa0, 0x52, 0x3b, 0xd6, 0xb3, 0x29, 0xe3, 0x2f, 0x84,
  0x53, 0xd1, 0x00, 0xed, 0x20, 0xfc, 0xb1, 0x5b, 0x6a, 0xcb, 0xbe, 0x39, 0x4a, 0x4c, 0x58, 0xcf,
  0xd0, 0xef, 0xaa, 0xfb, 0x43, 0x4d, 0x33, 0x85, 0x45, 0xf9, 0x02, 0x7f, 0x50, 0x3c, 0x9f, 0xa8,
  0x51, 0xa3, 0x40, 0x8f, 0x92, 0x9d, 0x38, 0xf5, 0xbc, 0xb6, 0xda, 0x21, 0x10, 0xff, 0xf3, 0xd2,
  0xcd, 0x0c, 0x13, 0xec, 0x5f, 0x97, 0x44, 0x17, 0xc4, 0xa7, 0x7e, 0x3d, 0x64, 0x5d, 0x19, 0x73,
  0x60, 0x81, 0x4f, 0xdc, 0x22, 0x2a, 0x90, 0x88, 0x46, 0xee, 0xb8, 0x14, 0xde, 0x5e, 0x0b, 0xdb,
  0xe0, 0x32, 0x3a, 0x0a, 0x49, 0x06, 0x24, 0x5c, 0xc2, 0xd3, 0xac, 0x62, 0x91, 0x95, 0xe4, 0x79,
  0xe7, 0xc8, 0x37, 0x6d, 0x8d, 0xd5, 0x4e, 0xa9, 0x6c, 0x56, 0xf4, 0xea, 0x65, 0x7a, 0xae, 0x08,
  0xba, 0x78, 0x25, 0x2e, 0x1c, 0xa6, 0xb4, 0xc6, 0xe8, 0xdd, 0x74, 0x1f, 0x4b, 0xbd, 0x8b, 0x8a,
  0x70, 0x3e, 0xb5, 0x66, 0x48, 0x03, 0xf6, 0x0e, 0x61, 0x35, 0x57, 0xb9, 0x86, 0xc1, 0x1d, 0x9e,
  0xe1, 0xf8, 0x98, 0x11, 0x69, 0xd9, 0x8e, 0x94, 0x9b, 0x1e, 0x87, 0xe9, 0xce, 0x55, 0x28, 0xdf,
  0x8c, 0xa1, 0x89, 0x0d, 0xbf, 0xe6, 0x42, 0x68, 0x41, 0x99, 0x2d, 0x0f, 0xb0, 0x54, 0xbb, 0x16};
permutation kalinaSB1{
  0xA8, 0x43, 0x5F, 0x06, 0x6B, 0x75, 0x6C, 0x59, 0x71, 0xDF, 0x87, 0x95, 0x17, 0xF0, 0xD8, 0x09,
  0x6D, 0xF3, 0x1D, 0xCB, 0xC9, 0x4D, 0x2C, 0xAF, 0x79, 0xE0, 0x97, 0xFD, 0x6F, 0x4B, 0x45, 0x39,
  0x3E, 0xDD, 0xA3, 0x4F, 0xB4, 0xB6, 0x9A, 0x0E, 0x1F, 0xBF, 0x15, 0xE1, 0x49, 0xD2, 0x93, 0xC6,
  0x92, 0x72, 0x9E, 0x61, 0xD1, 0x63, 0xFA, 0xEE, 0xF4, 0x19, 0xD5, 0xAD, 0x58, 0xA4, 0xBB, 0xA1,
  0xDC, 0xF2, 0x83, 0x37, 0x42, 0xE4, 0x7A, 0x32, 0x9C, 0xCC, 0xAB, 0x4A, 0x8F, 0x6E, 0x04, 0x27,
  0x2E, 0xE7, 0xE2, 0x5A, 0x96, 0x16, 0x23, 0x2B, 0xC2, 0x65, 0x66, 0x0F, 0xBC, 0xA9, 0x47, 0x41,
  0x34, 0x48, 0xFC, 0xB7, 0x6A, 0x88, 0xA5, 0x53, 0x86, 0xF9, 0x5B, 0xDB, 0x38, 0x7B, 0xC3, 0x1E,
  0x22, 0x33, 0x24, 0x28, 0x36, 0xC7, 0xB2, 0x3B, 0x8E, 0x77, 0xBA, 0xF5, 0x14, 0x9F, 0x08, 0x55,
```

```
  0x9B, 0x4C, 0xFE, 0x60, 0x5C, 0xDA, 0x18, 0x46, 0xCD, 0x7D, 0x21, 0xB0, 0x3F, 0x1B, 0x89, 0xFF,
  0xEB, 0x84, 0x69, 0x3A, 0x9D, 0xD7, 0xD3, 0x70, 0x67, 0x40, 0xB5, 0xDE, 0x5D, 0x30, 0x91, 0xB1,
  0x78, 0x11, 0x01, 0xE5, 0x00, 0x68, 0x98, 0xA0, 0xC5, 0x02, 0xA6, 0x74, 0x2D, 0x0B, 0xA2, 0x76,
  0xB3, 0xBE, 0xCE, 0xBD, 0xAE, 0xE9, 0x8A, 0x31, 0x1C, 0xEC, 0xF1, 0x99, 0x94, 0xAA, 0xF6, 0x26,
  0x2F, 0xEF, 0xE8, 0x8C, 0x35, 0x03, 0xD4, 0x7F, 0xFB, 0x05, 0xC1, 0x5E, 0x90, 0x20, 0x3D, 0x82,
  0xF7, 0xEA, 0x0A, 0x0D, 0x7E, 0xF8, 0x50, 0x1A, 0xC4, 0x07, 0x57, 0xB8, 0x3C, 0x62, 0xE3, 0xC8,
  0xAC, 0x52, 0x64, 0x10, 0xD0, 0xD9, 0x13, 0x0C, 0x12, 0x29, 0x51, 0xB9, 0xCF, 0xD6, 0x73, 0x8D,
  0x81, 0x54, 0xC0, 0xED, 0x4E, 0x44, 0xA7, 0x2A, 0x85, 0x25, 0xE6, 0xCA, 0x7C, 0x8B, 0x56, 0x80};

permutation kalinaSB2{
  0xCE, 0xBB, 0xEB, 0x92, 0xEA, 0xCB, 0x13, 0xC1, 0xE9, 0x3A, 0xD6, 0xB2, 0xD2, 0x90, 0x17, 0xF8,
  0x42, 0x15, 0x56, 0xB4, 0x65, 0x1C, 0x88, 0x43, 0xC5, 0x5C, 0x36, 0xBA, 0xF5, 0x57, 0x67, 0x8D,
  0x31, 0xF6, 0x64, 0x58, 0x9E, 0xF4, 0x22, 0xAA, 0x75, 0x0F, 0x02, 0xB1, 0xDF, 0x6D, 0x73, 0x4D,
  0x7C, 0x26, 0x2E, 0xF7, 0x08, 0x5D, 0x44, 0x3E, 0x9F, 0x14, 0xC8, 0xAE, 0x54, 0x10, 0xD8, 0xBC,
  0x1A, 0x6B, 0x69, 0xF3, 0xBD, 0x33, 0xAB, 0xFA, 0xD1, 0x9B, 0x68, 0x4E, 0x16, 0x95, 0x91, 0xEE,
  0x4C, 0x63, 0x8E, 0x5B, 0xCC, 0x3C, 0x19, 0xA1, 0x81, 0x49, 0x7B, 0xD9, 0x6F, 0x37, 0x60, 0xCA,
  0xE7, 0x2B, 0x48, 0xFD, 0x96, 0x45, 0xFC, 0x41, 0x12, 0x0D, 0x79, 0xE5, 0x89, 0x8C, 0xE3, 0x20,
  0x30, 0xDC, 0xB7, 0x6C, 0x4A, 0xB5, 0x3F, 0x97, 0xD4, 0x62, 0x2D, 0x06, 0xA4, 0xA5, 0x83, 0x5F,
  0x2A, 0xDA, 0xC9, 0x00, 0x7E, 0xA2, 0x55, 0xBF, 0x11, 0xD5, 0x9C, 0xCF, 0x0E, 0x0A, 0x3D, 0x51,
  0x7D, 0x93, 0x1B, 0xFE, 0xC4, 0x47, 0x09, 0x86, 0x0B, 0x8F, 0x9D, 0x6A, 0x07, 0xB9, 0xB0, 0x98,
  0x18, 0x32, 0x71, 0x4B, 0xEF, 0x3B, 0x70, 0xA0, 0xE4, 0x40, 0xFF, 0xC3, 0xA9, 0xE6, 0x78, 0xF9,
  0x8B, 0x46, 0x80, 0x1E, 0x38, 0xE1, 0xB8, 0xA8, 0xE0, 0x0C, 0x23, 0x76, 0x1D, 0x25, 0x24, 0x05,
  0xF1, 0x6E, 0x94, 0x28, 0x9A, 0x84, 0xE8, 0xA3, 0x4F, 0x77, 0xD3, 0x85, 0xE2, 0x52, 0xF2, 0x82,
  0x50, 0x7A, 0x2F, 0x74, 0x53, 0xB3, 0x61, 0xAF, 0x39, 0x35, 0xDE, 0xCD, 0x1F, 0x99, 0xAC, 0xAD,
  0x72, 0x2C, 0xDD, 0xD0, 0x87, 0xBE, 0x5E, 0xA6, 0xEC, 0x04, 0xC6, 0x03, 0x34, 0xFB, 0xDB, 0x59,
  0xB6, 0xC2, 0x01, 0xF0, 0x5A, 0xED, 0xA7, 0x66, 0x21, 0x7F, 0x8A, 0x27, 0xC7, 0xC0, 0x29, 0xD7};

permutation kalinaSB3{
  0x93, 0xD9, 0x9A, 0xB5, 0x98, 0x22, 0x45, 0xFC, 0xBA, 0x6A, 0xDF, 0x02, 0x9F, 0xDC, 0x51, 0x59,
  0x4A, 0x17, 0x2B, 0xC2, 0x94, 0xF4, 0xBB, 0xA3, 0x62, 0xE4, 0x71, 0xD4, 0xCD, 0x70, 0x16, 0xE1,
  0x49, 0x3C, 0xC0, 0xD8, 0x5C, 0x9B, 0xAD, 0x85, 0x53, 0xA1, 0x7A, 0xC8, 0x2D, 0xE0, 0xD1, 0x72,
  0xA6, 0x2C, 0xC4, 0xE3, 0x76, 0x78, 0xB7, 0xB4, 0x09, 0x3B, 0x0E, 0x41, 0x4C, 0xDE, 0xB2, 0x90,
  0x25, 0xA5, 0xD7, 0x03, 0x11, 0x00, 0xC3, 0x2E, 0x92, 0xEF, 0x4E, 0x12, 0x9D, 0x7D, 0xCB, 0x35,
  0x10, 0xD5, 0x4F, 0x9E, 0x4D, 0xA9, 0x55, 0xC6, 0xD0, 0x7B, 0x18, 0x97, 0xD3, 0x36, 0xE6, 0x48,
  0x56, 0x81, 0x8F, 0x77, 0xCC, 0x9C, 0xB9, 0xE2, 0xAC, 0xB8, 0x2F, 0x15, 0xA4, 0x7C, 0xDA, 0x38,
  0x1E, 0x0B, 0x05, 0xD6, 0x14, 0x6E, 0x6C, 0x7E, 0x66, 0xFD, 0xB1, 0xE5, 0x60, 0xAF, 0x5E, 0x33,
  0x87, 0xC9, 0xF0, 0x5D, 0x6D, 0x3F, 0x88, 0x8D, 0xC7, 0xF7, 0x1D, 0xE9, 0xEC, 0xED, 0x80, 0x29,
  0x27, 0xCF, 0x99, 0xA8, 0x50, 0x0F, 0x37, 0x24, 0x28, 0x30, 0x95, 0xD2, 0x3E, 0x5B, 0x40, 0x83,
  0xB3, 0x69, 0x57, 0x1F, 0x07, 0x1C, 0x8A, 0xBC, 0x20, 0xEB, 0xCE, 0x8E, 0xAB, 0xEE, 0x31, 0xA2,
  0x73, 0xF9, 0xCA, 0x3A, 0x1A, 0xFB, 0x0D, 0xC1, 0xFE, 0xFA, 0xF2, 0x6F, 0xBD, 0x96, 0xDD, 0x43,
  0x52, 0xB6, 0x08, 0xF3, 0xAE, 0xBE, 0x19, 0x89, 0x32, 0x26, 0xB0, 0xEA, 0x4B, 0x64, 0x84, 0x82,
  0x6B, 0xF5, 0x79, 0xBF, 0x01, 0x5F, 0x75, 0x63, 0x1B, 0x23, 0x3D, 0x68, 0x2A, 0x65, 0xE8, 0x91,
  0xF6, 0xFF, 0x13, 0x58, 0xF1, 0x47, 0x0A, 0x7F, 0xC5, 0xA7, 0xE7, 0x61, 0x5A, 0x06, 0x46, 0x44,
  0x42, 0x04, 0xA0, 0xDB, 0x39, 0x86, 0x54, 0xAA, 0x8C, 0x34, 0x21, 0x8B, 0xF8, 0x0C, 0x74, 0x67};
```

```
permutation kalinaSB4{
  0x68, 0x8D, 0xCA, 0x4D, 0x73, 0x4B, 0x4E, 0x2A, 0xD4, 0x52, 0x26, 0xB3, 0x54, 0x1E, 0x19, 0x1F,
  0x22, 0x03, 0x46, 0x3D, 0x2D, 0x4A, 0x53, 0x83, 0x13, 0x8A, 0xB7, 0xD5, 0x25, 0x79, 0xF5, 0xBD,
  0x58, 0x2F, 0x0D, 0x02, 0xED, 0x51, 0x9E, 0x11, 0xF2, 0x3E, 0x55, 0x5E, 0xD1, 0x16, 0x3C, 0x66,
  0x70, 0x5D, 0xF3, 0x45, 0x40, 0xCC, 0xE8, 0x94, 0x56, 0x08, 0xCE, 0x1A, 0x3A, 0xD2, 0xE1, 0xDF,
  0xB5, 0x38, 0x6E, 0x0E, 0xE5, 0xF4, 0xF9, 0x86, 0xE9, 0x4F, 0xD6, 0x85, 0x23, 0xCF, 0x32, 0x99,
  0x31, 0x14, 0xAE, 0xEE, 0xC8, 0x48, 0xD3, 0x30, 0xA1, 0x92, 0x41, 0xB1, 0x18, 0xC4, 0x2C, 0x71,
  0x72, 0x44, 0x15, 0xFD, 0x37, 0xBE, 0x5F, 0xAA, 0x9B, 0x88, 0xD8, 0xAB, 0x89, 0x9C, 0xFA, 0x60,
  0xEA, 0xBC, 0x62, 0x0C, 0x24, 0xA6, 0xA8, 0xEC, 0x67, 0x20, 0xDB, 0x7C, 0x28, 0xDD, 0xAC, 0x5B,
  0x34, 0x7E, 0x10, 0xF1, 0x7B, 0x8F, 0x63, 0xA0, 0x05, 0x9A, 0x43, 0x77, 0x21, 0xBF, 0x27, 0x09,
  0xC3, 0x9F, 0xB6, 0xD7, 0x29, 0xC2, 0xEB, 0xC0, 0xA4, 0x8B, 0x8C, 0x1D, 0xFB, 0xFF, 0xC1, 0xB2,
  0x97, 0x2E, 0xF8, 0x65, 0xF6, 0x75, 0x07, 0x04, 0x49, 0x33, 0xE4, 0xD9, 0xB9, 0xD0, 0x42, 0xC7,
  0x6C, 0x90, 0x00, 0x8E, 0x6F, 0x50, 0x01, 0xC5, 0xDA, 0x47, 0x3F, 0xCD, 0x69, 0xA2, 0xE2, 0x7A,
  0xA7, 0xC6, 0x93, 0x0F, 0x0A, 0x06, 0xE6, 0x2B, 0x96, 0xA3, 0x1C, 0xAF, 0x6A, 0x12, 0x84, 0x39,
  0xE7, 0xB0, 0x82, 0xF7, 0xFE, 0x9D, 0x87, 0x5C, 0x81, 0x35, 0xDE, 0xB4, 0xA5, 0xFC, 0x80, 0xEF,
  0xCB, 0xBB, 0x6B, 0x76, 0xBA, 0x5A, 0x7D, 0x78, 0x0B, 0x95, 0xE3, 0xAD, 0x74, 0x98, 0x3B, 0x36,
  0x64, 0x6D, 0xDC, 0xF0, 0x59, 0xA9, 0x4C, 0x17, 0x7F, 0x91, 0xB8, 0xC9, 0x57, 0x1B, 0xE0, 0x61};
int main(){
  int n(8);
  auto data = experiment(saferSBI, n);
  distribution(data, n);
  std::cout << parkTheorem(data, n, 10) << std::endl;
  std::cout << "done" << std::endl;
  std::cin.get();
  std::cin.get();
}
```

ДОДАТОК Б ГРАФІКИ РОЗПОДІЛІВ УЗАГАЛЬНЕНИХ ЛІНІЙНИХ ПОТЕНЦІАЛІВ

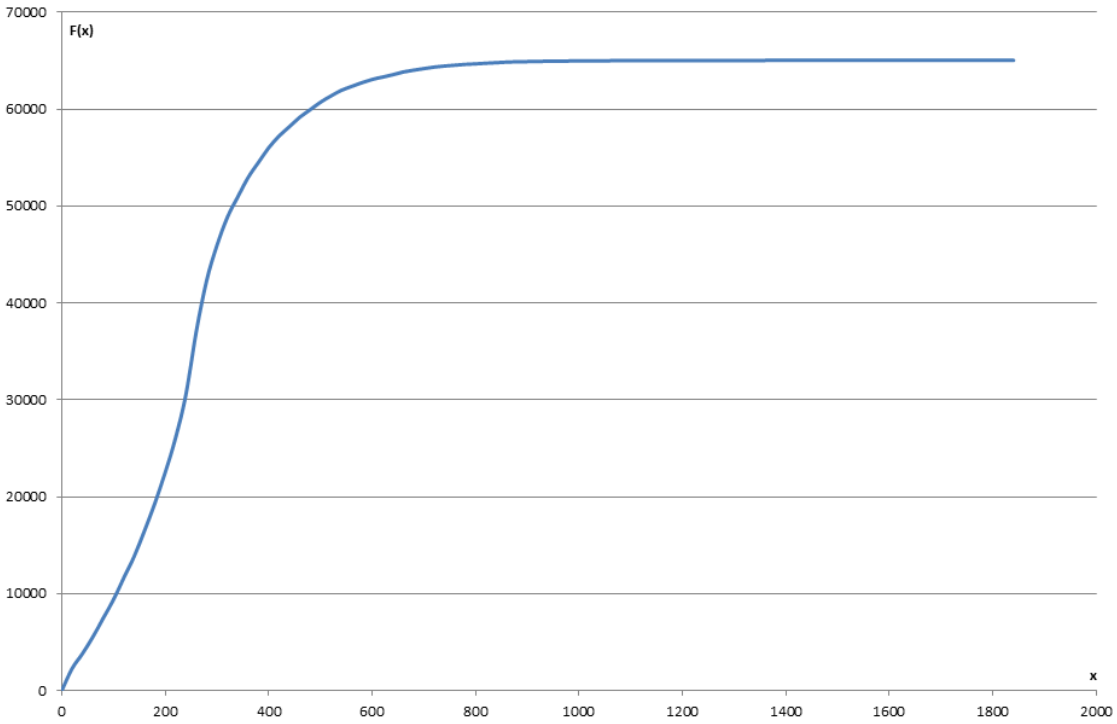

Рисунок Б.1 – SAFER

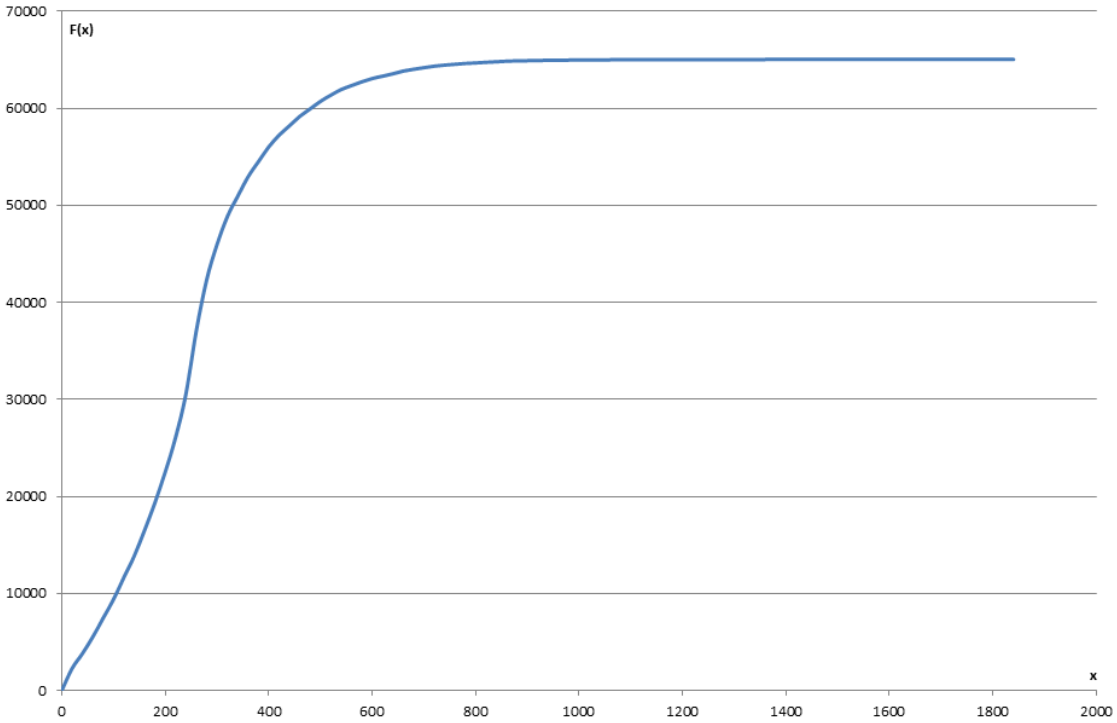

Рисунок Б.2 – SAFERInv

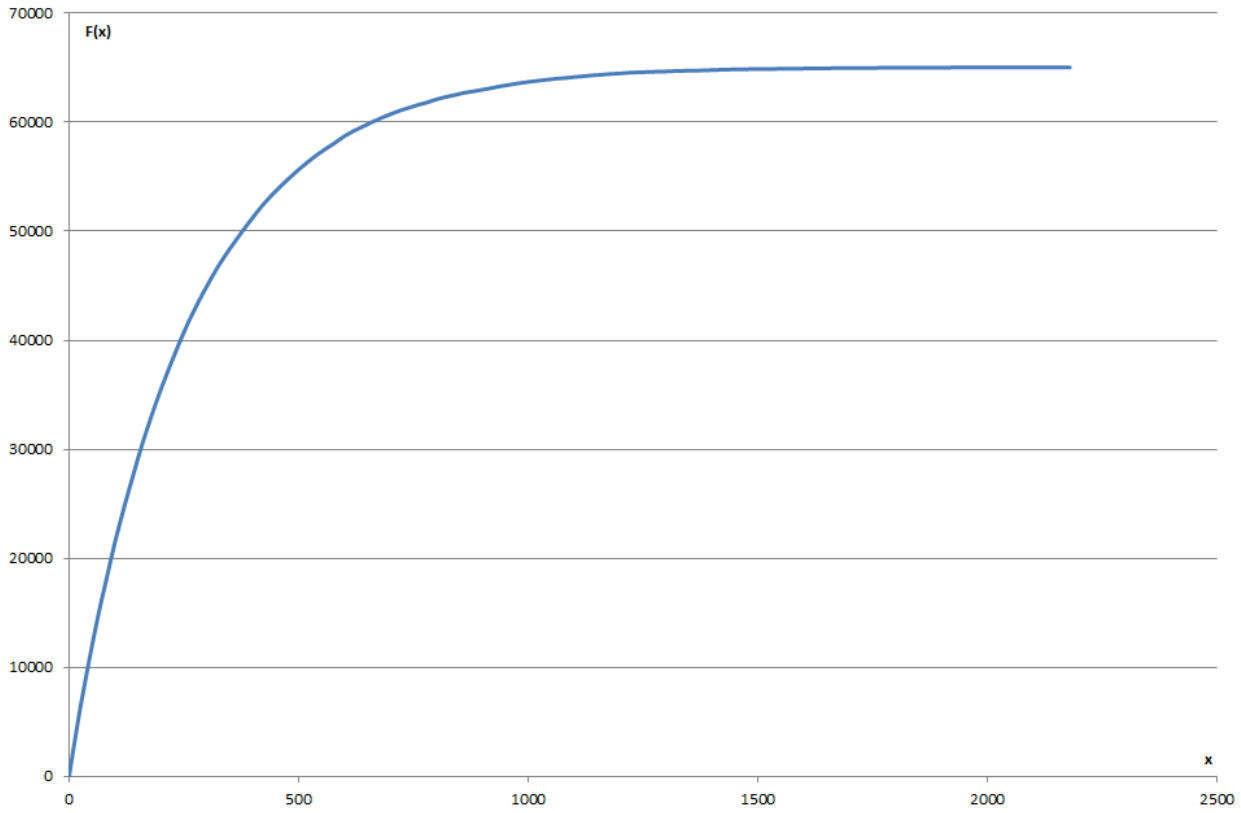

Рисунок Б.3 – Калина1

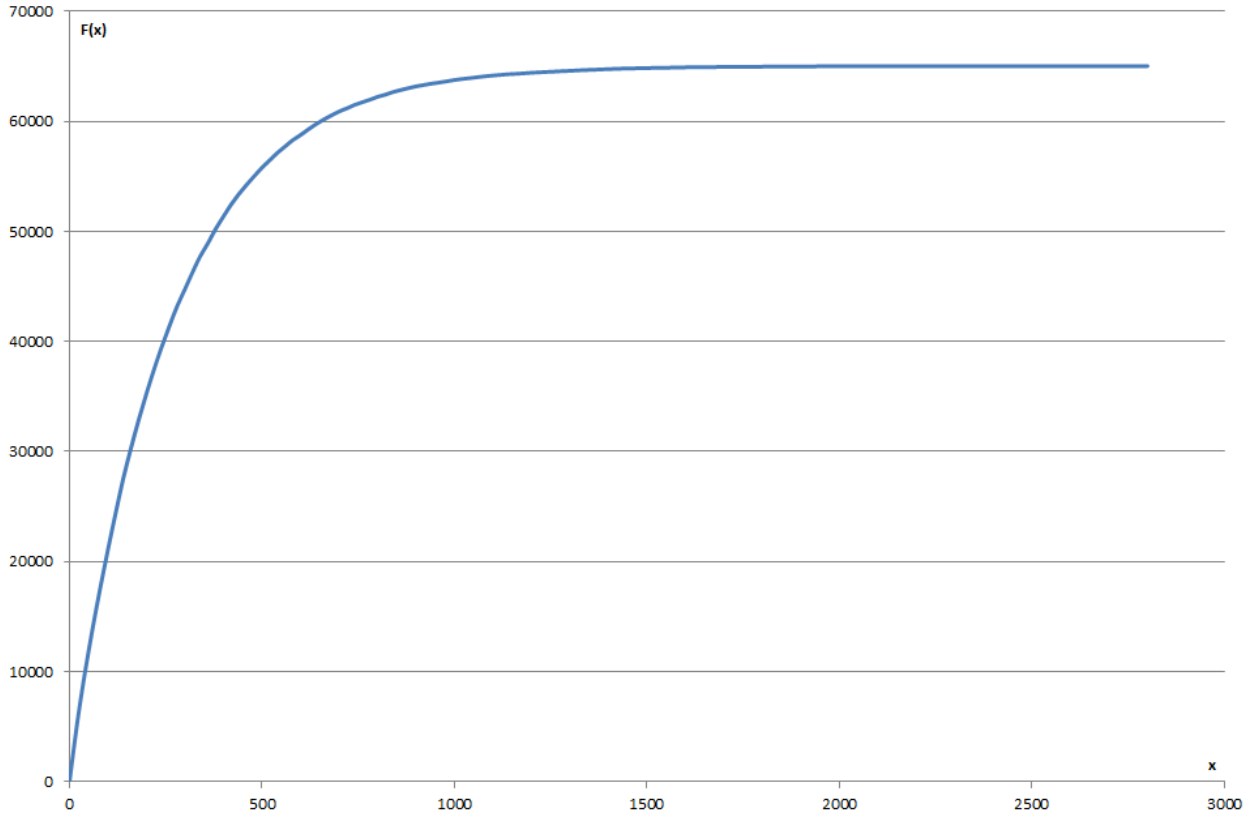

Рисунок Б.4 – Калина2

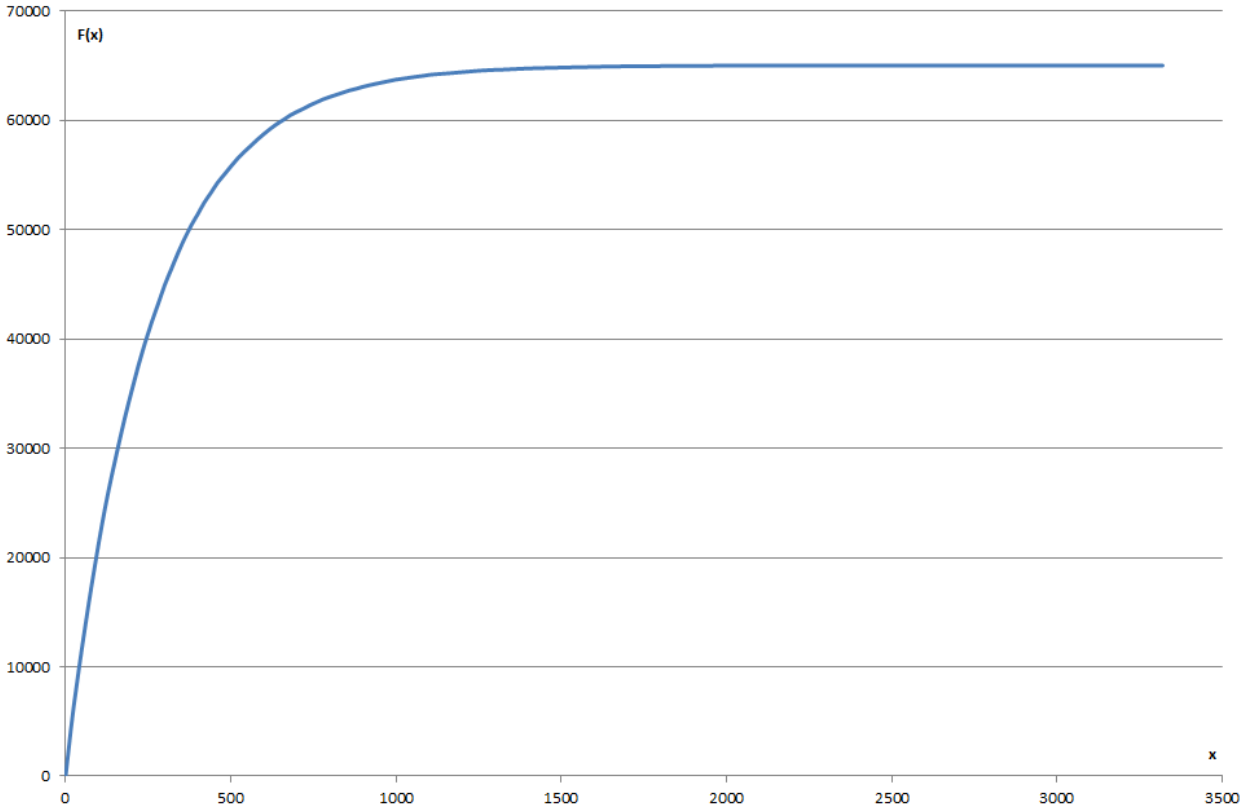

Рисунок Б.5 – Калина3

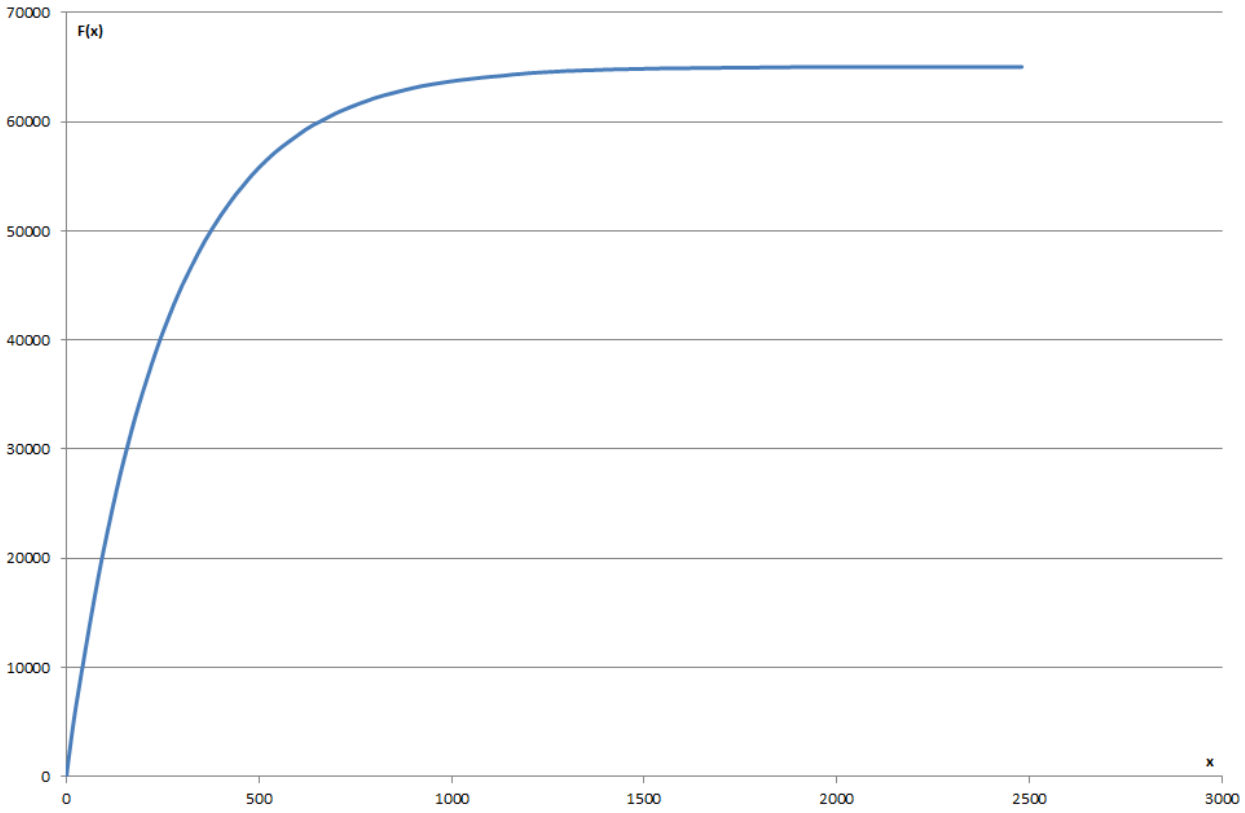

Рисунок Б.6 – Калина4